INFORME LABORATORIO CAMUOFLAGE Y BADBLUE

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

INFORME LABORATORIO CAMUOFLAGE Y BADBLUE

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

CONTENIDO

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

LISTA DE ILUSTRACIONES

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

INTRODUCCIÓN

El presente informe expone el desarrollo del laboratorio compuesto por dos capítulos, realizados en entornos virtuales mediante los sistemas operativos Kali Linux y Windows XP. El propósito central de este trabajo es analizar herramientas y técnicas orientadas a la seguridad en redes.

En el primer capítulo, se empleó la herramienta Camouflage en el sistema Windows XP para llevar a cabo el proceso de ocultamiento de archivos dentro de un portador de imagen, con el fin de determinar su capacidad y límites respecto al tipo, número y tamaño de los archivos camuflados. El segundo capítulo se enfocó en la explotación del servicio BadBlue a través del puerto HTTP (80), evaluando su funcionamiento y las implicaciones de seguridad derivadas de su uso. Para este propósito, se utilizó la utilidad Netcat (Ncat), la cual permitió establecer sesiones remotas entre las máquinas virtuales de Kali Linux y Windows XP.

Durante el desarrollo del laboratorio, se configuró una carpeta compartida en el equipo anfitrión, desde la cual se transfirieron los instaladores de las herramientas utilizadas. También, se llevaron a cabo los procedimientos de instalación, prueba y verificación, documentando cada paso de manera ordenada. Estas actividades permitieron comprender de forma práctica la interacción entre sistemas operativos, los riesgos asociados al manejo de información oculta y la importancia de aplicar medidas preventivas en entornos de red, fortaleciendo así los conocimientos en seguridad informática.

PLANTEAMIENTO DEL PROBLEMA

Se identifican dos retos principales que requieren verificación mediante el desarrollo del laboratorio: por un lado, determinar hasta qué punto la herramienta Camouflage permite ocultar diferentes tipos y cantidades de archivos dentro de un portador; por otro lado, comprobar si es posible establecer comunicación desde Kali Linux a Windows XP a través del servicio web BadBlue que opera en el puerto HTTP (80).

Universidad Tecnológica del Chocó
Diego Luis Córdoba

OBJETIVOS

General: Desarrollar y documentar, paso a paso, los procedimientos realizados durante la ejecución del laboratorio.

Específicos:

- Realizar la configuración e instalación de carpetas compartidas en VirtualBox.
- Realizar la instalación de las aplicaciones en Windows XP (BadBlue, /Adobe, Camouflage, Edge)
- Usar Camouflage como método para camuflar archivos.
- Verificar la conectividad y acceso a BadBlue en XP.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 CAPÍTULO 1: CAMOUFLAGE

El proceso se inició con la apertura del programa **VirtualBox** desde el equipo host. En la siguiente imagen se observa la disposición general de la ventana: en el panel lateral izquierdo aparecen las máquinas virtuales existentes; se encuentra seleccionada la máquina virtual Windows XP, y en la parte superior de la interfaz se visualiza la barra de comandos con las opciones **Nueva**, **Añadir**, **Configuración**, **Descartar** y **Mostrar/Iniciar.**

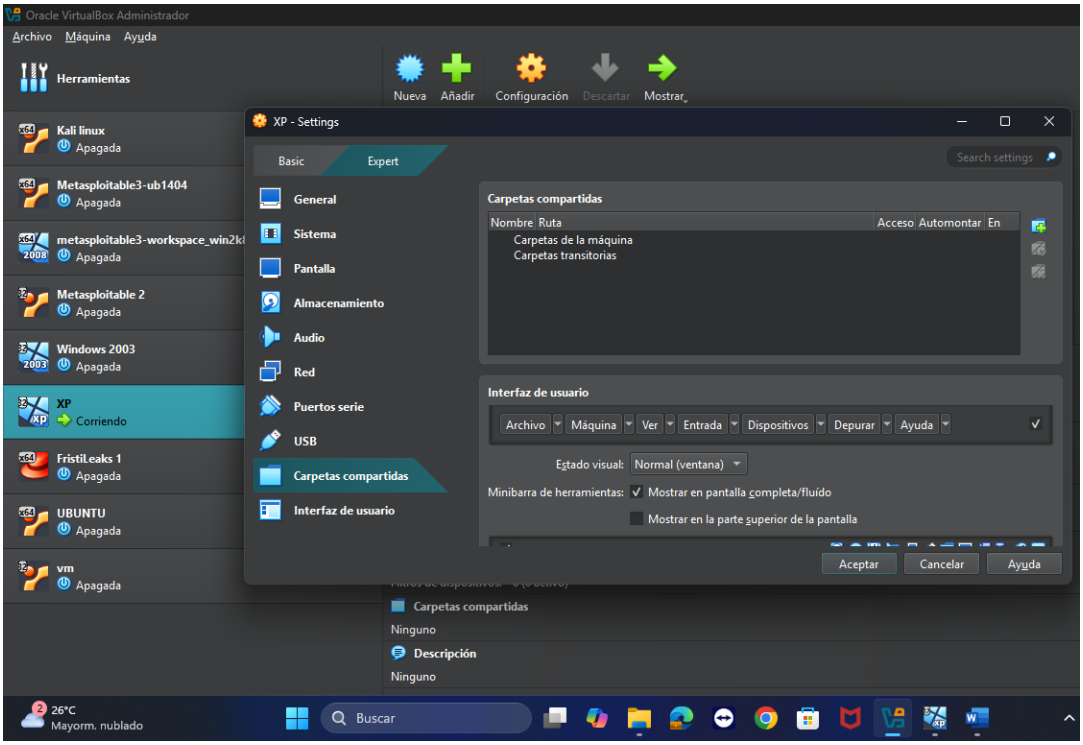


Ilustración 1 Pestaña Carpetas Compartidas XP

Al seleccionar la opción Configuración, se carga una nueva ventana que contiene los distintos apartados configurables para la máquina seleccionada, General, Almacenamiento, Red, entre otros... Dentro de esta ventana se ubica la sección **Carpetas compartidas**, la cual despliega una vista donde se listan las carpetas actualmente configuradas (en este caso, no existía ninguna aún).

En esta pestaña se muestran dos columnas: **Nombre** y **Ruta**, correspondientes a las carpetas compartidas establecidas. En la parte lateral derecha se encuentran tres iconos funcionales: **añadir carpeta**, **editar/mover** y **eliminar**. Desde el primero de ellos se procedió a crear la carpeta compartida necesaria para el laboratorio.

Para ello, se realizó clic en el icono con el + ubicado en la parte lateral derecha de la ventana.

Al hacerlo, se despliega una pequeña ventana de configuración que permite definir los parámetros de la carpeta a compartir. En esta se especifica la ruta del directorio en el equipo anfitrión, el nombre de la carpeta, el punto de montaje dentro de la máquina virtual y las opciones Solo lectura, Automontar y Hacer permanente.

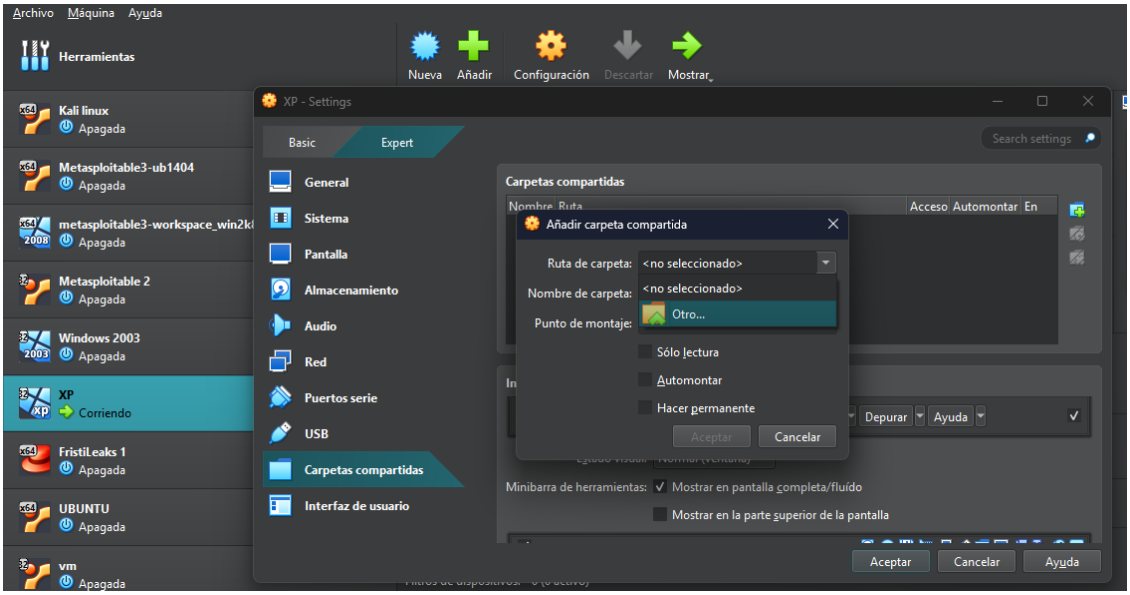


Ilustración 2 Ventana añadir carpeta

Como no se identifica de forma inmediata la ruta exacta del directorio a compartir, se selecciono el icono  ubicado en la parte lateral izquierda de la pestaña y, posteriormente, el icono de carpeta **Otro**…, el cual permitio abrir el explorador de archivos del sistema host.

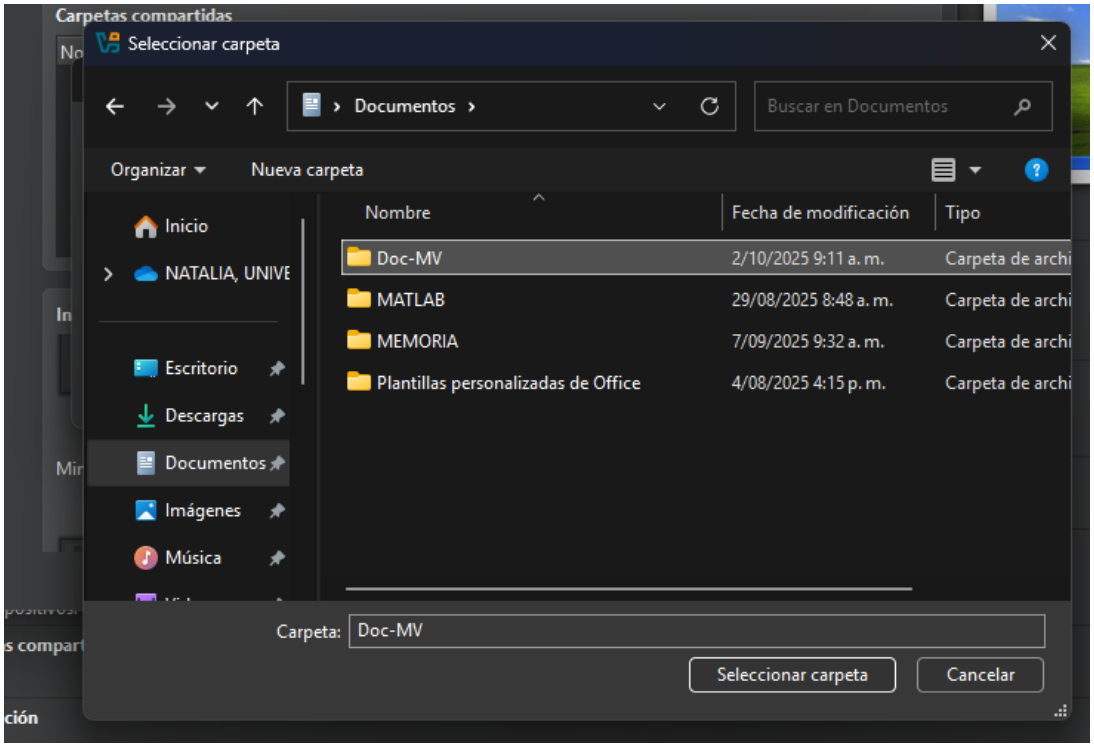
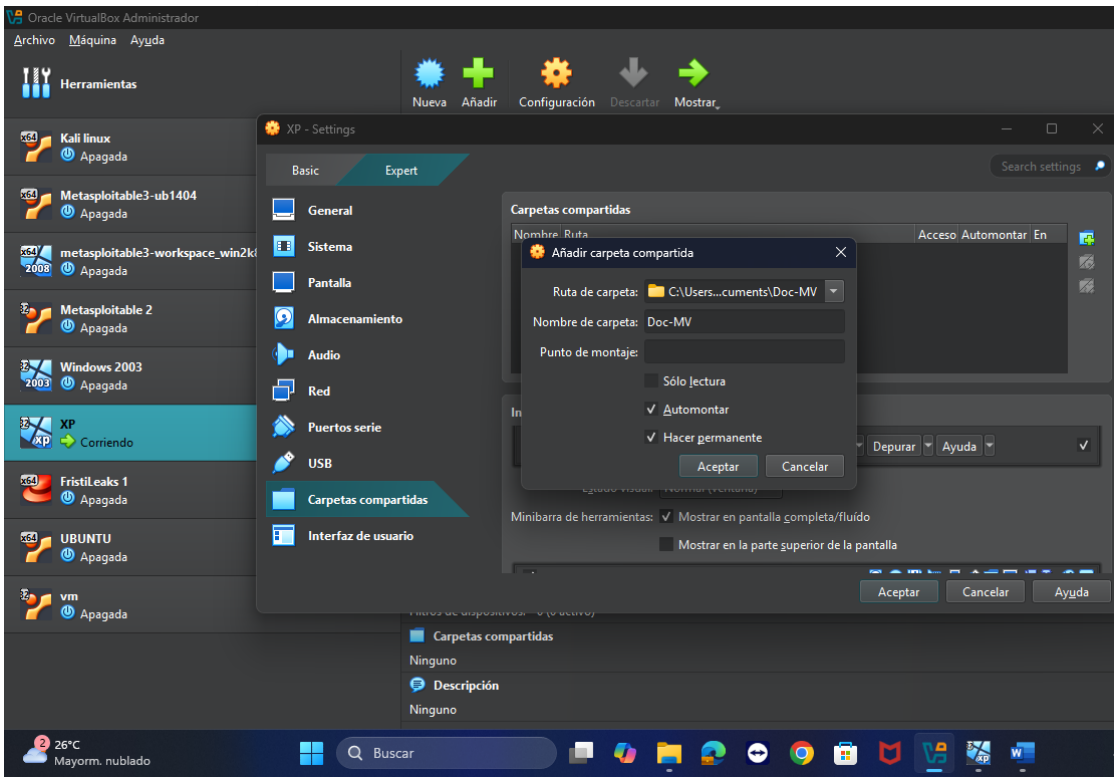


Ilustración 3 Selección de carpeta compartida

En esta imagen se puede observar la ventana emergente que muestra las carpetas disponibles en el equipo host. Desde esta interfaz, se seleccionó la carpeta a compartir, en este caso **Doc-MV** de la lista mostrada y, a continuación, se realiza clic en el botón Seleccionar carpeta para confirmar la elección.

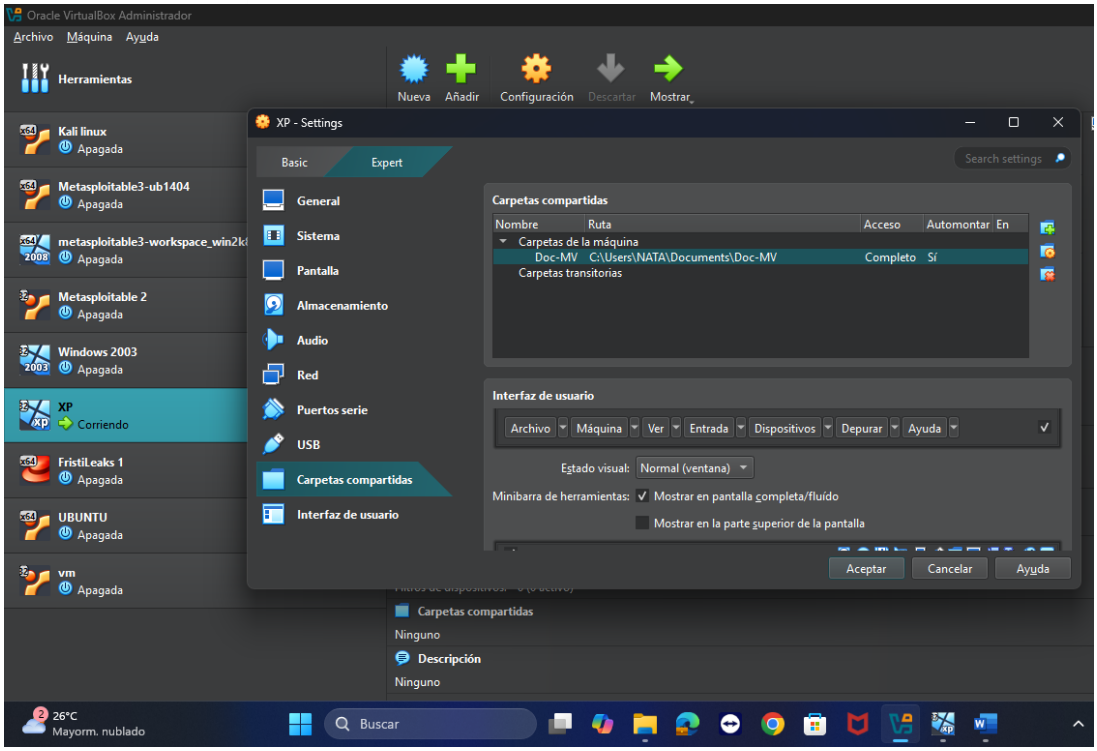
Una vez realizada esta acción, el sistema retorno automáticamente a la ventana anterior de configuración de carpetas compartidas.



Donde se visualizó la ruta de la carpeta seleccionada y el nombre asignado de forma automática por VirtualBox. En esta misma ventana se habilitaron las opciones de configuración adicionales. Se recomendó por parte del docente marcar las casillas **Automontar y Hacer permanente**, de modo que la carpeta se monte de forma automática cada vez que se inicie la máquina virtual y permanezca configurada para futuros usos.

Con la configuración finalizada, se realizó clic en el botón **Aceptar** para guardar los cambios y regresar al menú principal de la máquina virtual, dejando lista la carpeta compartida para ser reconocida dentro de Windows XP una vez se inicie la sesión.

En la siguiente captura se muestra que la carpeta se ha añadido correctamente:



El siguiente paso consistió en aceptar los cambios realizados en la configuración de la máquina virtual XP, asegurando que la carpeta compartida quede correctamente registrada dentro de VirtualBox.

Una vez guardada la configuración, se inició la máquina virtual Windows XP para continuar con el proceso, para ello, tenido seleccionada la máquina se realizó clic en la opción Iniciar del menú superior de VirtualBox. Durante el arranque, en la barra superior de la máquina virtual XP, se carga un nuevo menú donde se encuentran las opciones: Archivo, Maquina, Ver Entrada, Dispositivos, Ayuda… se accede al menú Dispositivos y se selecciona la opción **Insertar imagen de CD de los complementos de los invitados** en las opciones de la nueva vista. En la siguiente imagen se observa la selección:

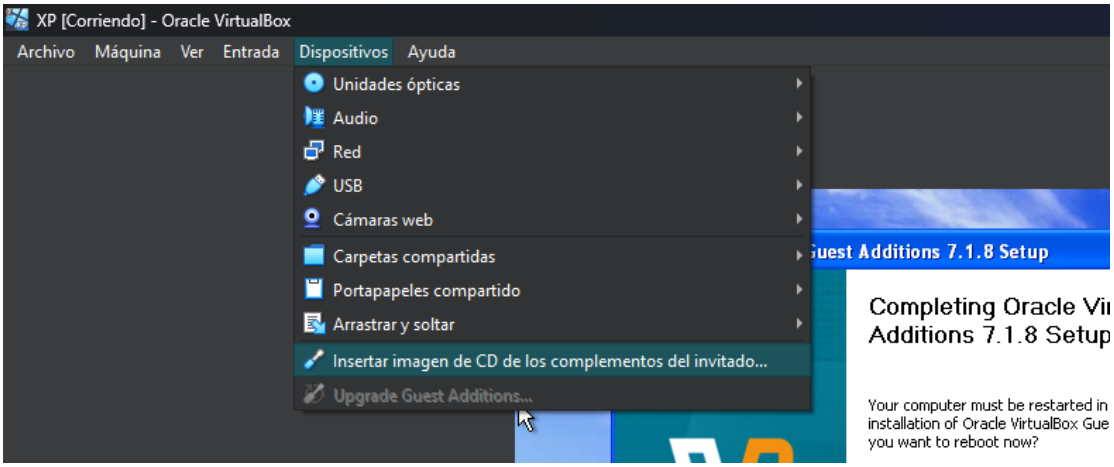


Ilustración 4 Insertar imagen de CD de los complementos de los invitados

Esta acción monta automáticamente en el sistema Windows XP una unidad de CD virtual que contiene las herramientas necesarias para mejorar la compatibilidad entre el host y la máquina virtual, especialmente, la habilitación del acceso a carpetas compartidas.

Una vez cargada la máquina, dentro del sistema Windows XP, se accede al menú **Inicio > Mi PC**, donde se pueden visualizar las diferentes unidades disponibles en el equipo. En esta sección, se localiza un nuevo dispositivo identificado como **Virtual Guest Additions (D),** el cual aparece como una unidad de almacenamiento extraíble.

Esta unidad corresponde a la imagen de CD virtual que VirtualBox inserta automáticamente cuando se selecciona la opción Insertar imagen de CD de los complementos de los invitados. Observar la siguiente imagen:

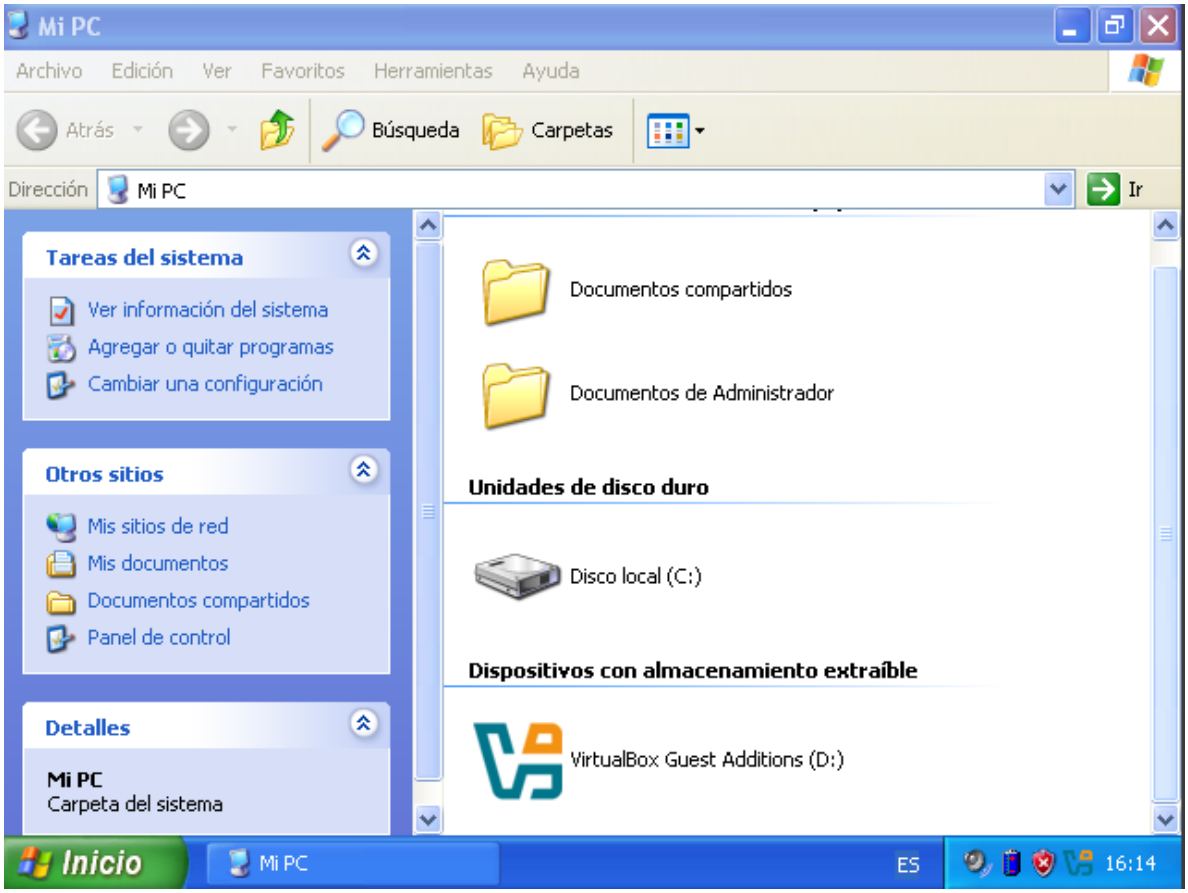


Ilustración 5 almacenamiento extraíble Virtual Guest Additions (D)

El proceso siguiente consiste en ejecutar el instalador de Guest Additions desde la unidad Virtual Guest Additions (D) y seguir el asistente paso a paso. Al abrir el instalador, se presenta la pantalla inicial del asistente; en este punto se selecciona **Next** para continuar la secuencia de instalación. En la siguiente secuencia de imágenes, se presenta el proceso de instalación:

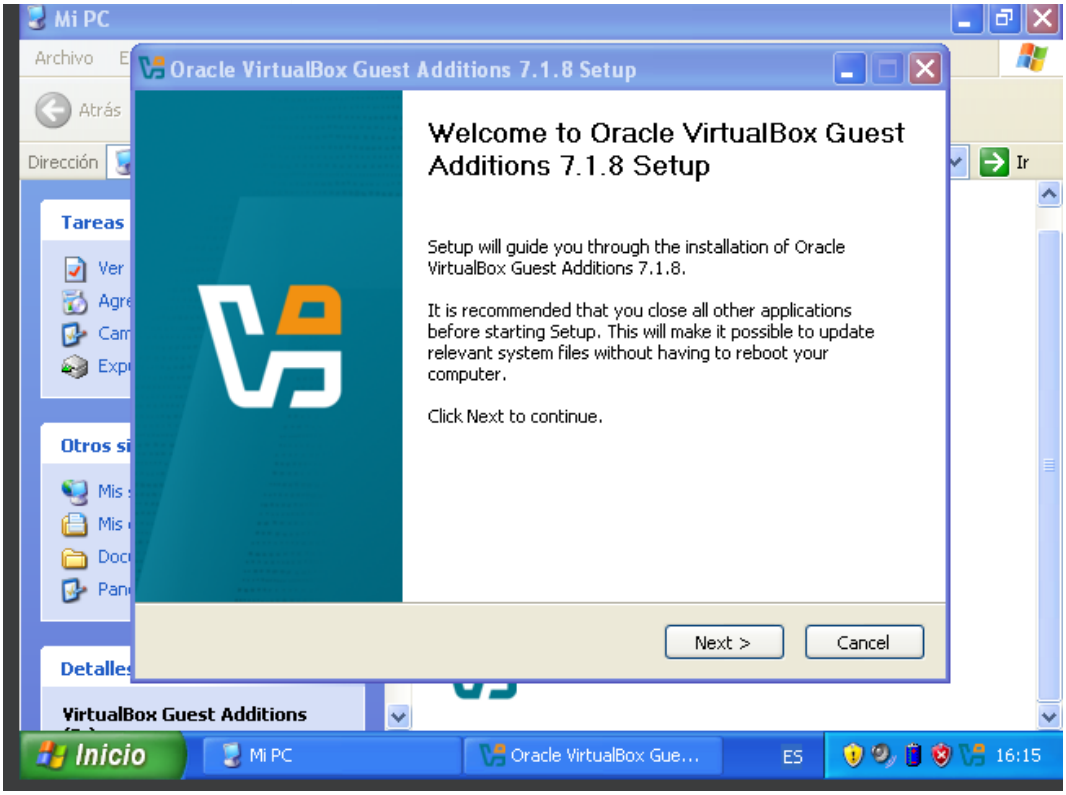


Ilustración 6 Instalación almacenamiento extraíble Virtual Guest Additions (D)

Esta es la primera vista del instalador, la cual corresponde a la pantalla inicial del asistente de instalación. En esta ventana se presenta la bienvenida al proceso y se muestran brevemente las funciones que se instalarán en el sistema. Se procede al siguiente paso haciendo clic en el botón Next, ubicado en la parte inferior de la ventana, y conduce a la siguiente etapa del asistente.

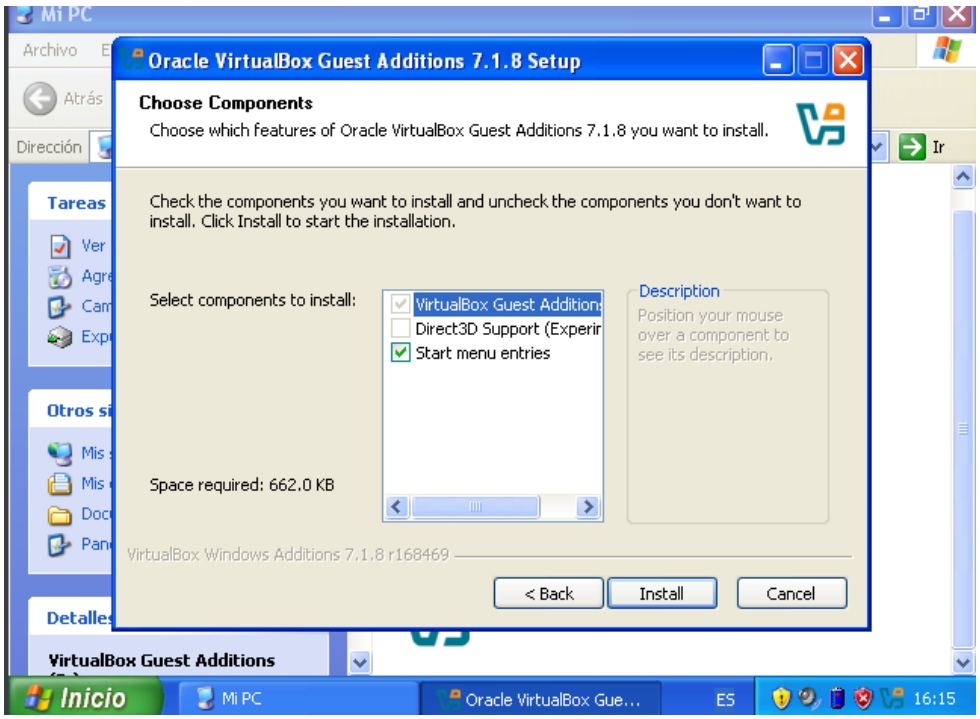


Ilustración 7 Instalacion de componentes

Esta es la segunda ventana del asistente de instalación, en la cual se presentan los componentes que serán instalados en el sistema. El instalador permite seleccionar o desmarcar las funciones adicionales que se desean incluir, en este caso, se dejaron las opciones predeterminadas. Una vez verificado que las casillas necesarias permanecían marcadas, se procedió a continuar con el proceso haciendo clic en el botón **Install,** ubicado en la parte inferior de la ventana. Con esta acción, el instalador comenzó a copiar los archivos y a configurar los componentes seleccionados dentro del sistema operativo Windows XP.

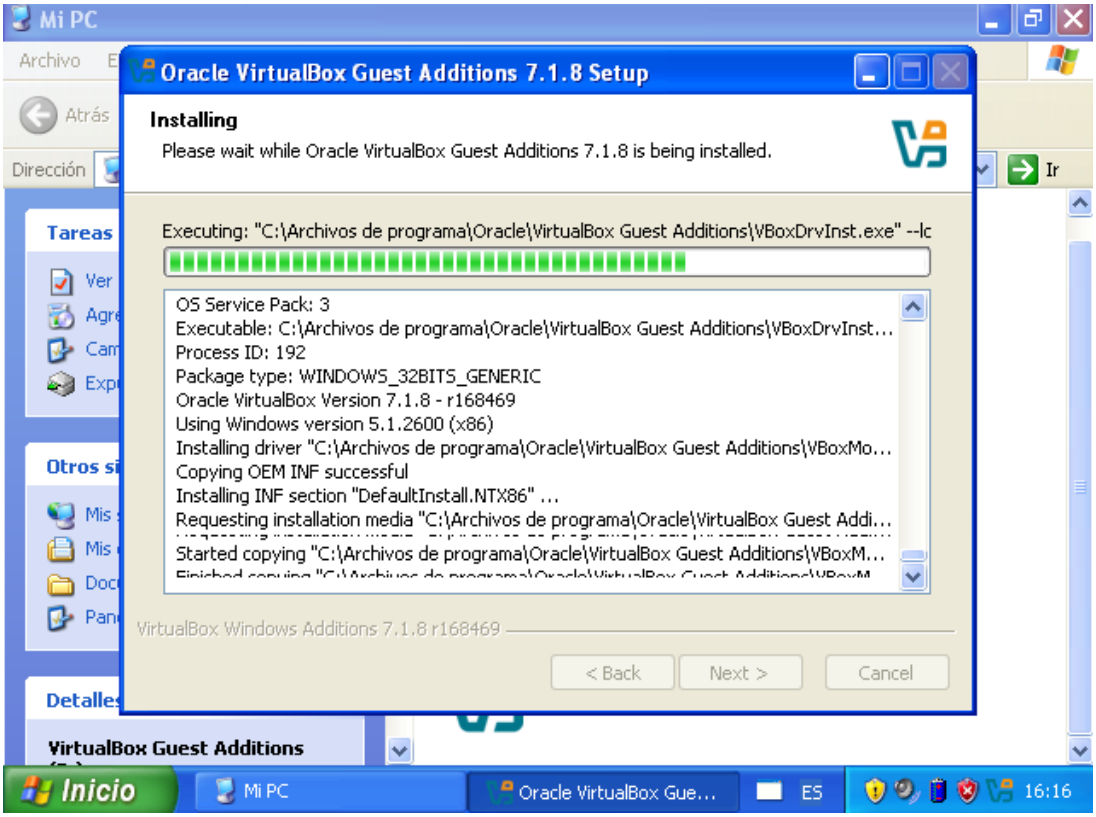


Ilustración 8 Finalización de instalación almacenamiento extraíble Virtual Guest Additions (D)

En esta ventana se observó el progreso de la instalación, representado mediante una barra de avance que indica el porcentaje completado del proceso. Aquí, el sistema copia los archivos necesarios y realiza la configuración de los componentes seleccionados previamente.

Se esperó hasta que la barra de progreso alcanzara el 100%, momento en el cual el instalador finalizó la transferencia de archivos y la integración del programa en el sistema Windows XP. Una vez completado este paso, el asistente avanzó automáticamente hacia la siguiente ventana, indicando que la instalación se había realizado con éxito.

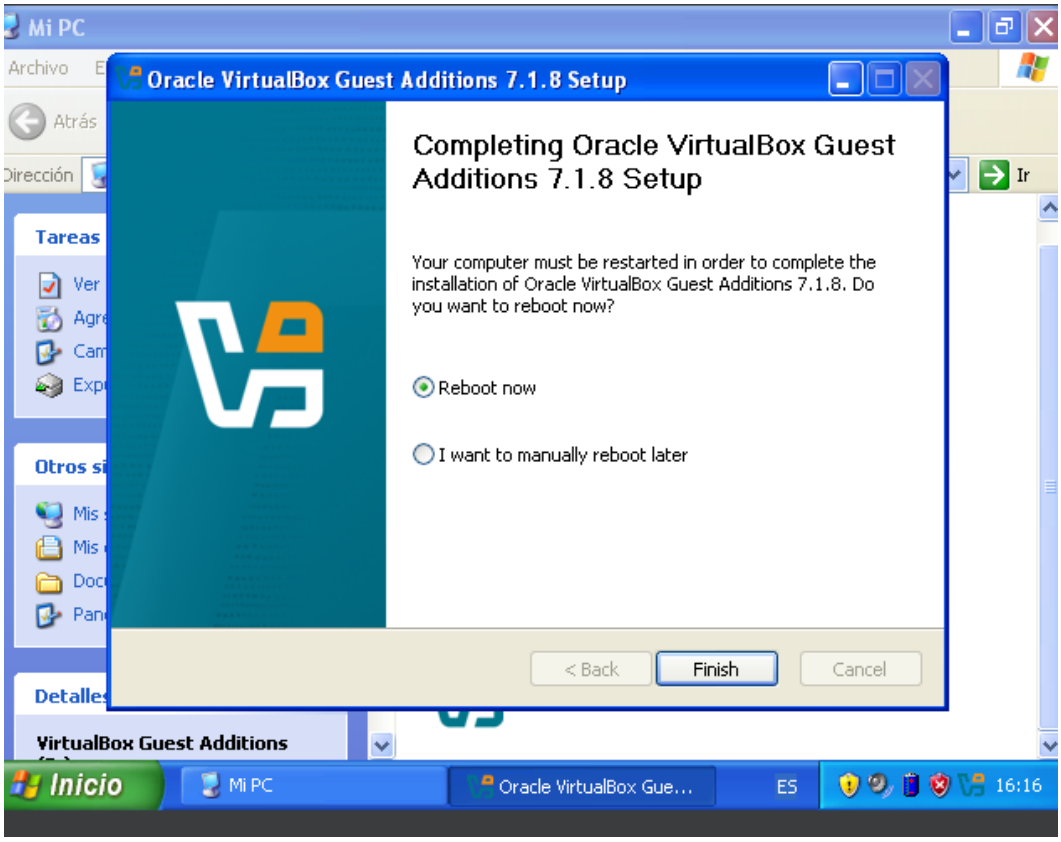


Ilustración 9 Confirmación de instalación

Una vez finalizada la transferencia de archivos y la configuración de los servicios, el asistente mostro la pantalla de completado. En esta etapa, se marcó la opción de reinicio y finalizar con **Finish.** El reinicio de Windows XP asegura que los controladores y servicios de Guest Additions queden correctamente cargados en el siguiente inicio del sistema.

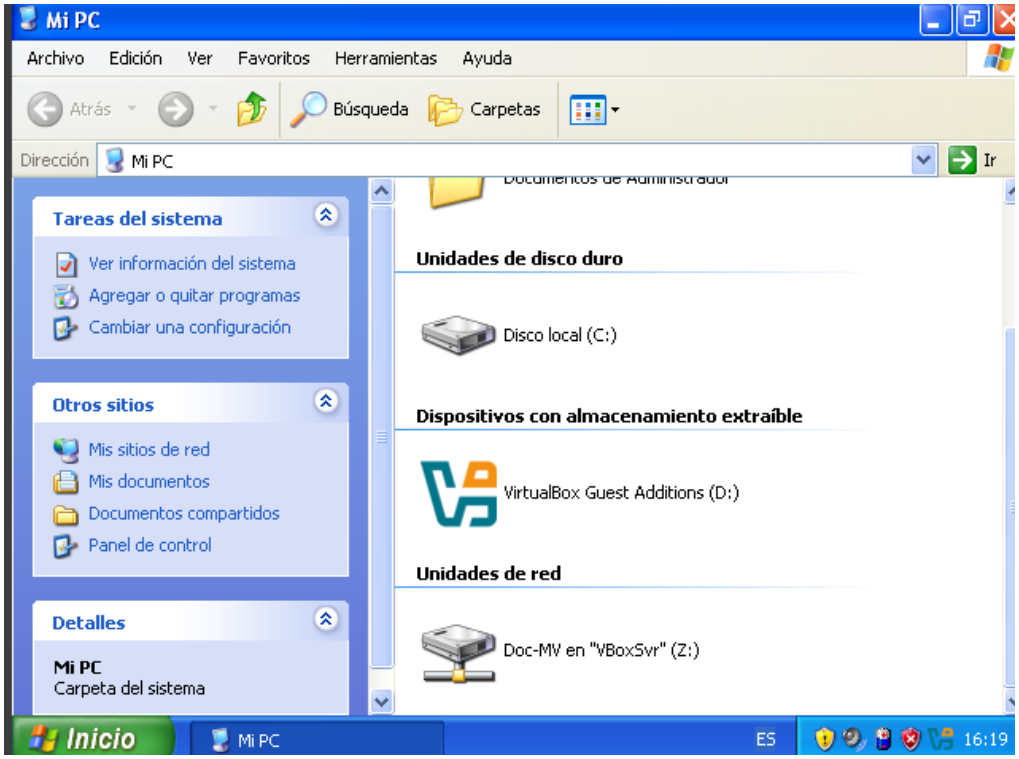


Ilustración 10 Visualización de carpeta compartida

Tras el reinicio, se verifico que el acceso a carpetas compartidas estuviera disponible, para ello se accede al menú **Inicio, Mi PC**, y como se observa en la imagen la carpeta compartida **Doc-MV** está disponible, lo que confirma que la instalación se llevó a cabo de forma satisfactoria.

En el equipo host, dentro de la carpeta previamente configurada como compartida, se **agregaron los archivos necesarios para la práctica**, tales como instaladores y documentos requeridos durante el desarrollo del laboratorio.

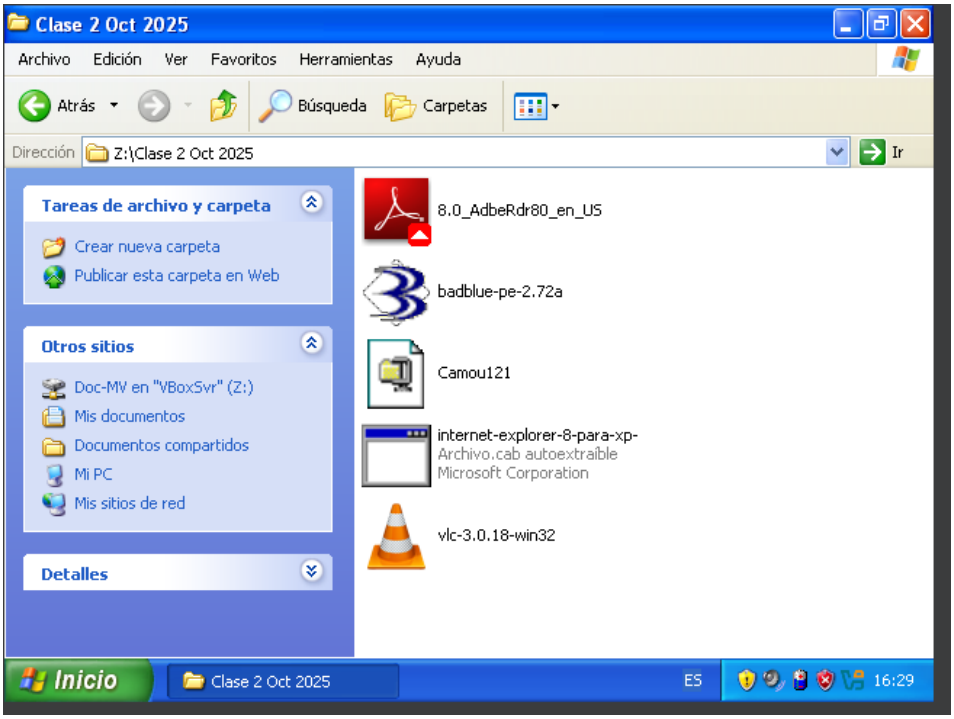


Ilustración 11 Archivos a instalar XP

Una vez copiados los archivos en dicha carpeta, se procedió a verificar su visualización en Windows XP. Para ello, dentro de XP se accedió a **Inicio, Mi PC**, donde se ubicó la unidad de red correspondiente a la carpeta compartida creada anteriormente.

Al hacer clic sobre esta unidad, en esta ventana se mostró el **contenido sincronizado desde el host**, permitiendo comprobar que el intercambio de archivos entre ambos sistemas se encontraba habilitado.

Los elementos visibles en la carpeta compartida correspondían a los instaladores de las herramientas utilizadas en el laboratorio: BadBlue Personal Edition, Camouflage, Adobe Reader 8, Microsoft Edge, VLC Media Player.

Los archivos se copiaron al escritorio de XP y posteriormente se procedió con su instalación, la siguiente secuencia de imágenes muestra el proceso de instalación de cada uno de ellos:

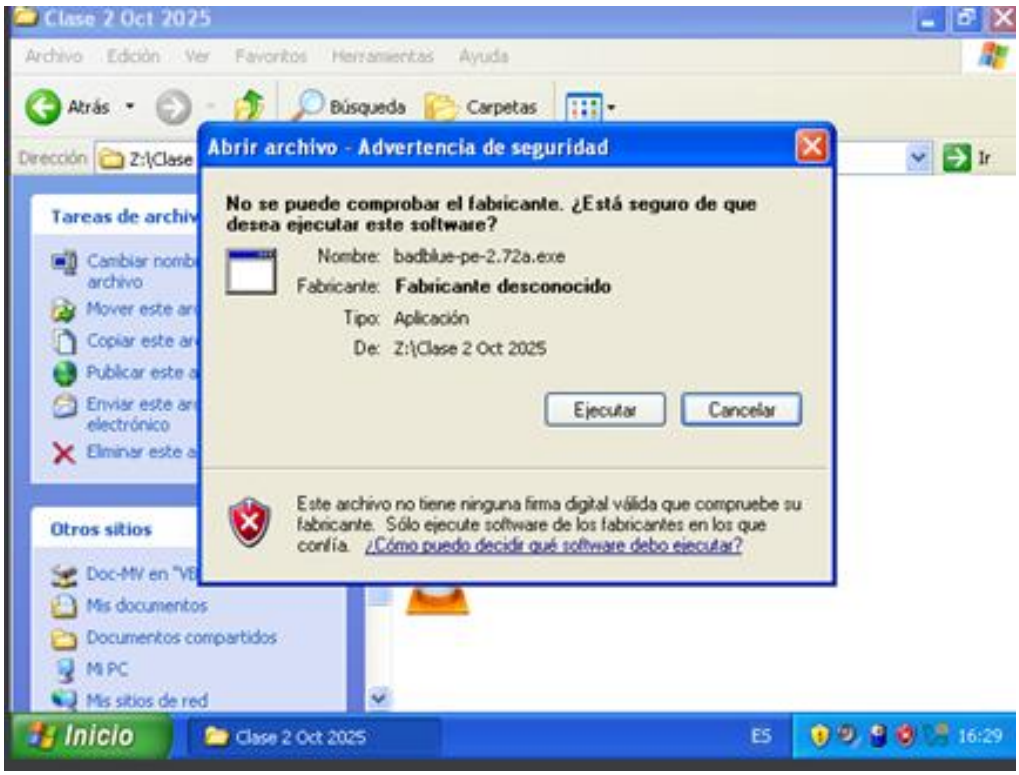


Ilustración 12 Instalación BadBlue

Al ejecutar el archivo instalador de BadBlue, se cargó esta ventana de advertencia de seguridad del sistema operativo, en la cual se solicita confirmación para continuar con la instalación. El mensaje indica si el usuario está seguro de ejecutar el archivo, ya que proviene de una fuente externa. Luego, se seleccionó la opción Ejecutar para autorizar el proceso y el asistente de BadBlue comenzó a copiar los archivos necesarios y a configurar los

componentes del servicio web en Windows XP. El procedimiento continuo hasta que se completó la instalación.

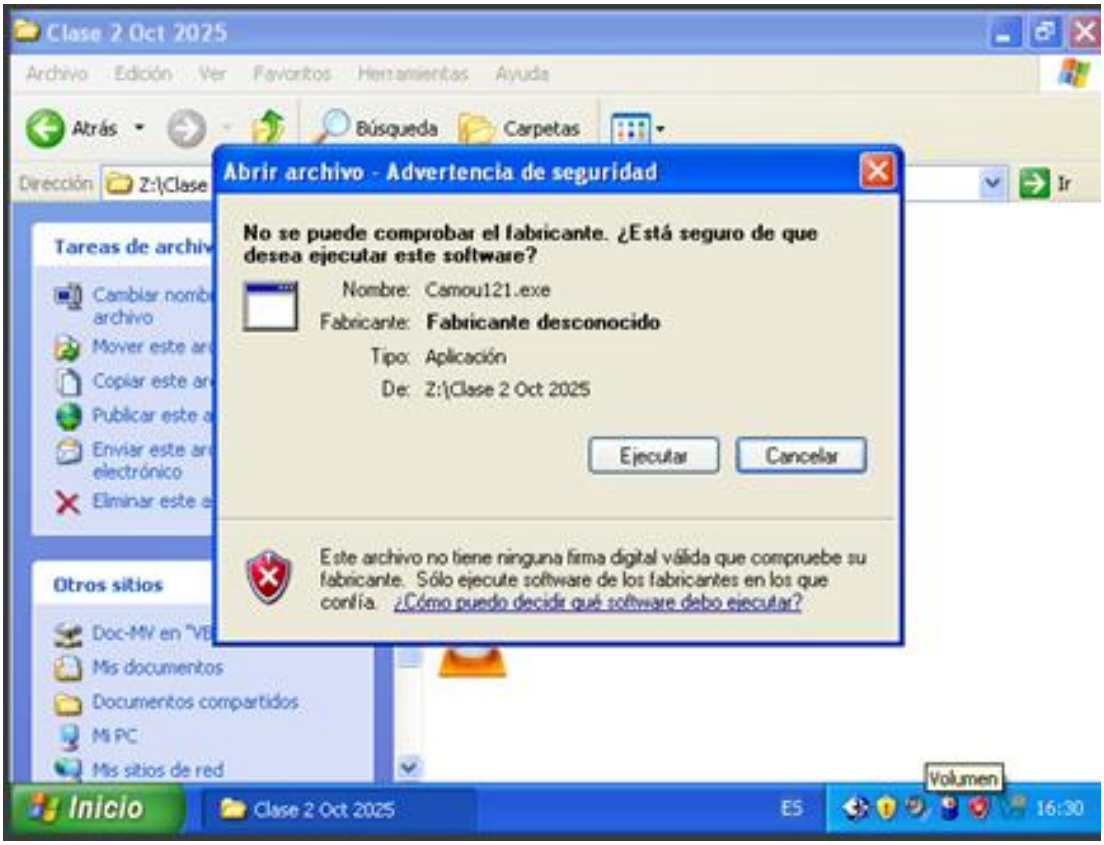


Ilustración 13 Instalación de Camouflage

Se repitió el mismo proceso de instalación: se ejecutó el archivo del programa, el sistema mostró una advertencia de seguridad, y se procedió a autorizar la ejecución seleccionando la opción Ejecutar para continuar con la instalación.

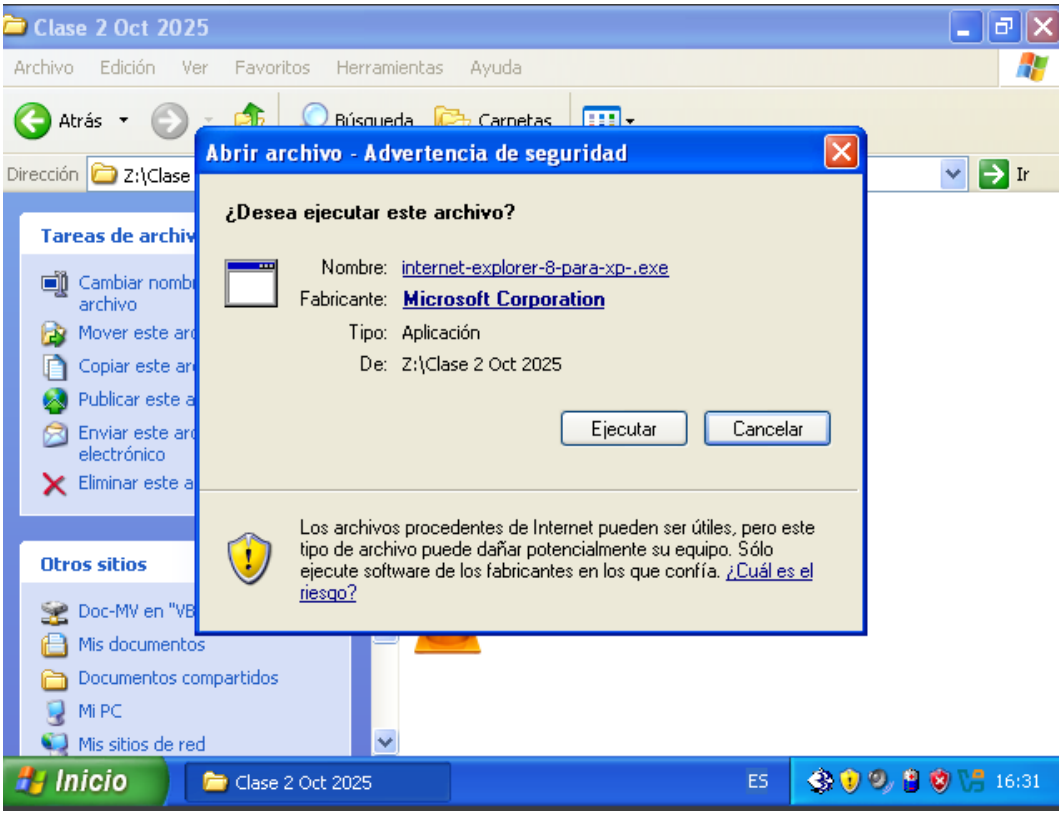


Ilustración 14 Instalación de Microsoft Edge

Se repitió el mismo proceso de instalación: se ejecutó el archivo del programa, el sistema mostró una advertencia de seguridad, y se procedió a autorizar la ejecución seleccionando la opción Ejecutar para continuar con la instalación.

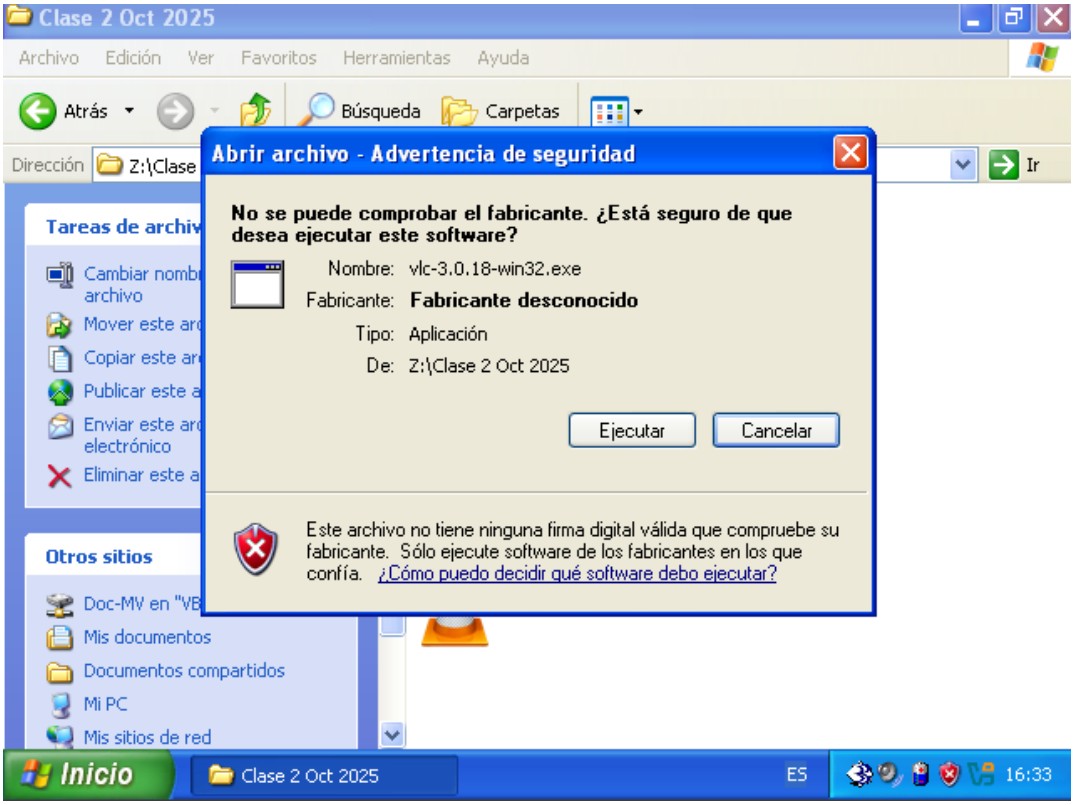


Ilustración 15 Instalación de VLC

Se repitió el mismo proceso de instalación: se ejecutó el archivo del programa, el sistema mostró una advertencia de seguridad, y se procedió a autorizar la ejecución seleccionando la opción Ejecutar para continuar con la instalación.

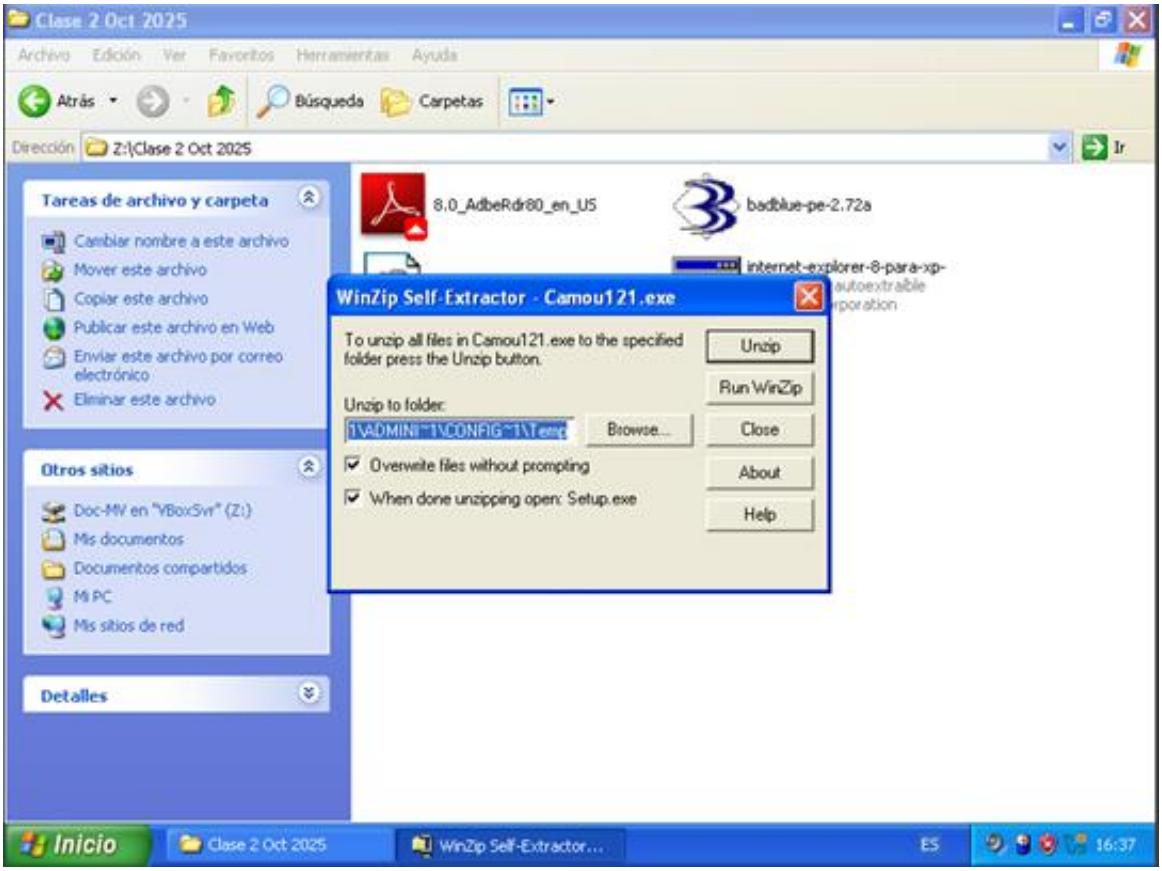


Ilustración 16 Instalación de Camouflage

Para la instalación de Camouflage, como se observa en la imagen, fue necesario descomprimir el archivo instalador utilizando la opción **Unzip**. Una vez extraídos los archivos, se ejecutó el instalador principal y se siguieron los pasos del asistente, avanzando con las opciones predeterminadas hasta que la instalación finalizó correctamente.

Ilustración 17 Escritorio XP

Una vez finalizada la instalación de los programas, se pudo observar en el escritorio de Windows XP los accesos directos correspondientes a cada una de las aplicaciones instaladas. Esto permitió verificar que la instalación se completó correctamente y que todos los programas quedaron disponibles para su uso dentro del entorno virtual.

El siguiente paso consistió en el uso de la herramienta Camouflage. Para ello, se compartieron tres archivos desde la carpeta compartida del equipo anfitrión hacia la máquina virtual con Windows XP.

.

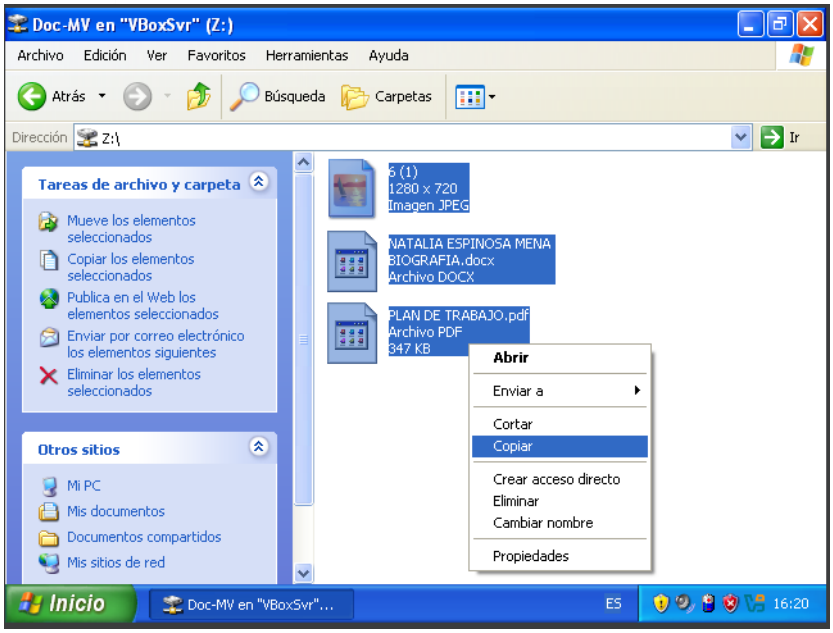
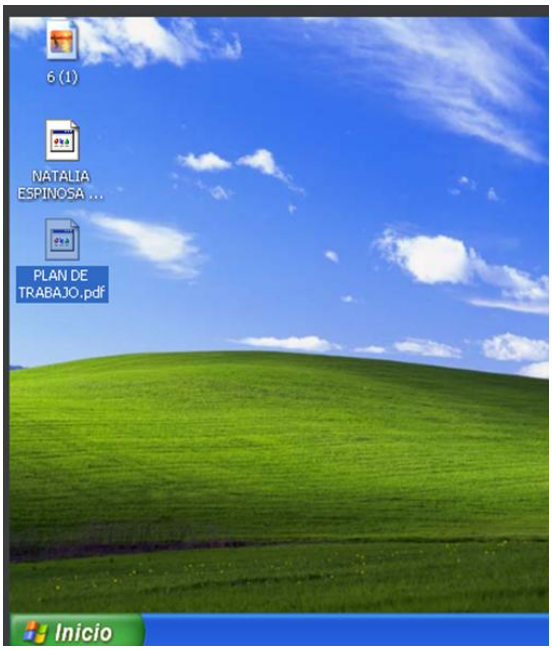


Ilustración 18 Archivos compartidos

Los archivos correspondían a una imagen (.jpg), un documento PDF (.pdf) y un archivo de Word (.docx).

Una vez transferidos, los archivos fueron copiados al escritorio de XP para facilitar su manipulación durante la práctica, tal como se muestra en las imágenes.



La imagen fue utilizada como archivo portador para realizar el proceso de camuflaje. Antes de iniciar la incrustación de los archivos, se procedió a verificar el peso original de esta, con el fin de contar con un valor de referencia que permitiera comparar posteriormente el cambio de tamaño tras el proceso de ocultamiento.

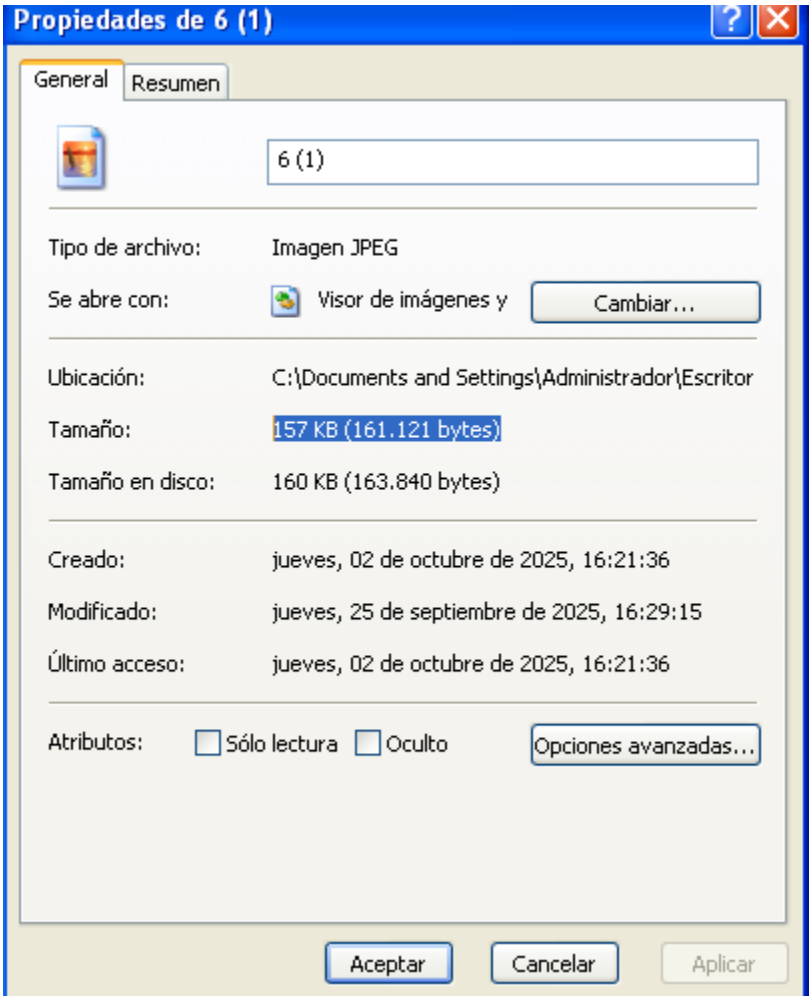


Ilustración 20 Verificación del peso de la imagen

Dentro de la imagen seleccionada como archivo portador, se procedió a camuflar los archivos PDF y DOCX. Para ello, se seleccionaron ambos archivos, y posteriormente se hizo clic derecho, desplegando el menú contextual del sistema.

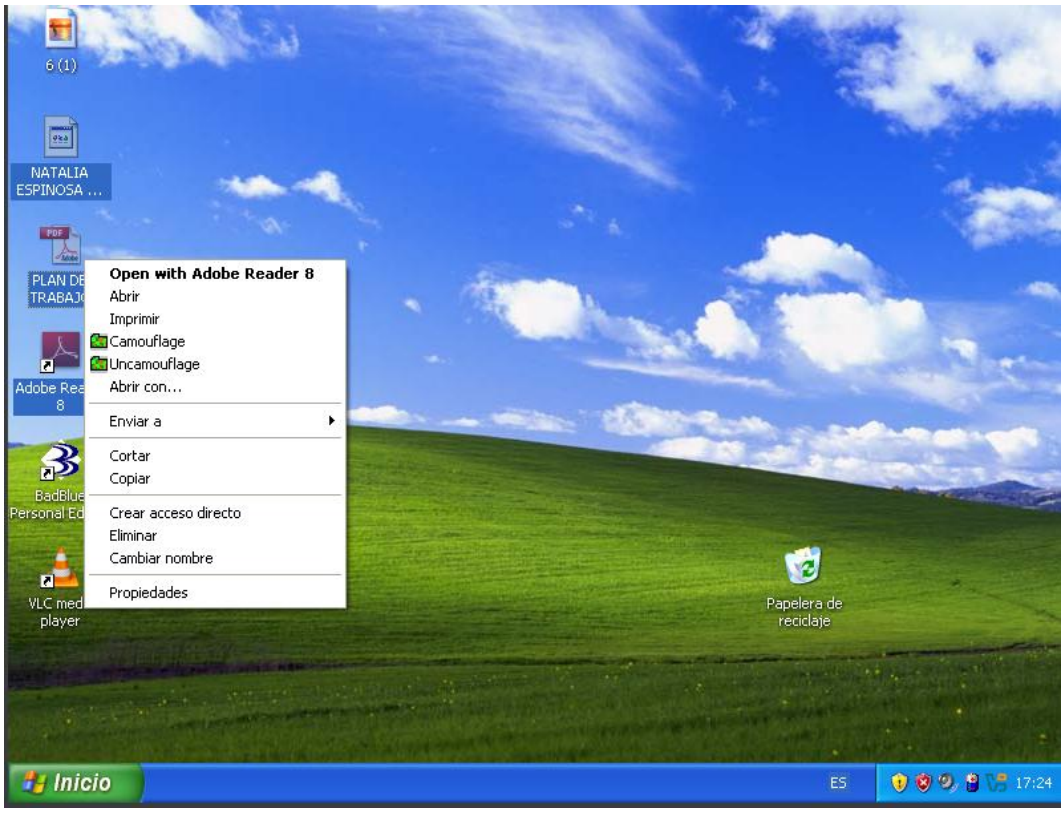


Ilustración 21 Camuflaje de Archivos

Entre las opciones disponibles, se eligió **Camouflage,** lo que inició una secuencia de pasos guiados que permiten incorporar los archivos seleccionados dentro de la imagen, proceso que se detalla a continuación.

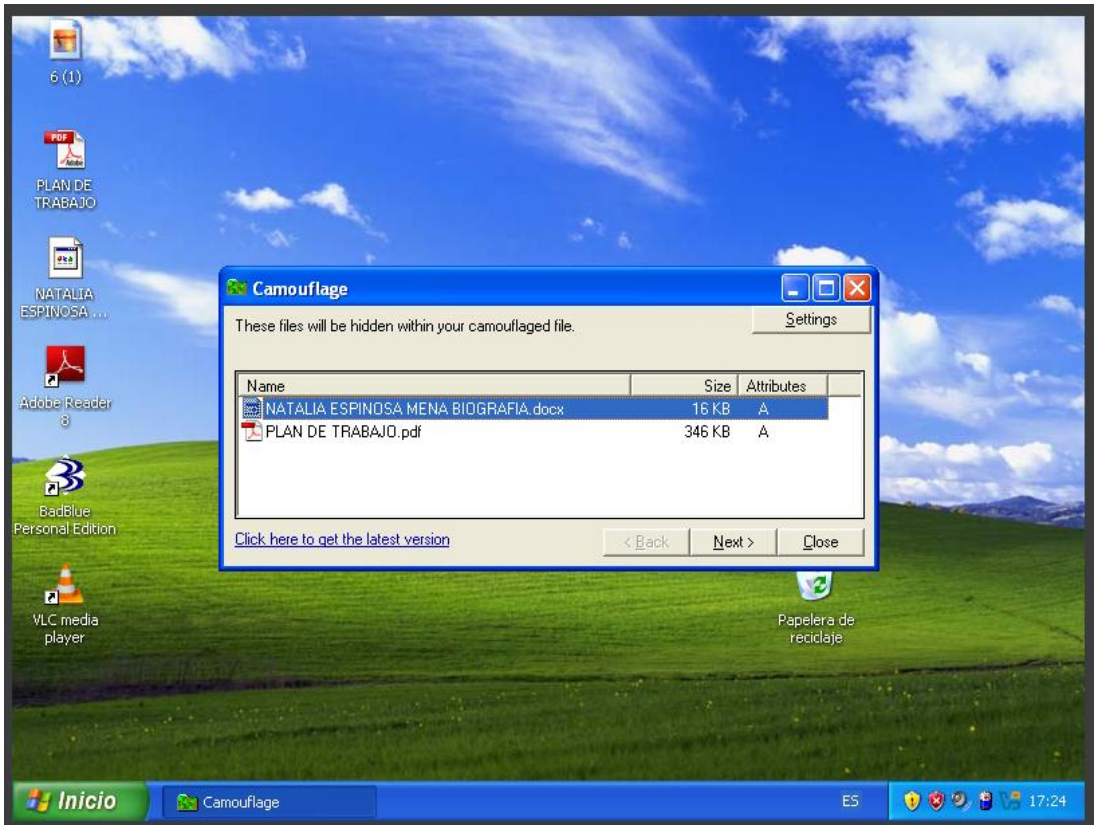


Ilustración 22 Archivos seleccionados a camuflar

Esta ventana pertenece al programa Camouflage y aparece de forma automática después de seleccionar la opción Camouflage. En esta interfaz se muestran los archivos previamente seleccionados que serán camuflados dentro del archivo portador, permitiendo verificar que la selección sea correcta antes de continuar con el proceso, el proceso continuo al presionar el botón **Next.**

En las siguientes dos imágenes, se muestra el archivo que seleccionado para camuflar los dos archivos:

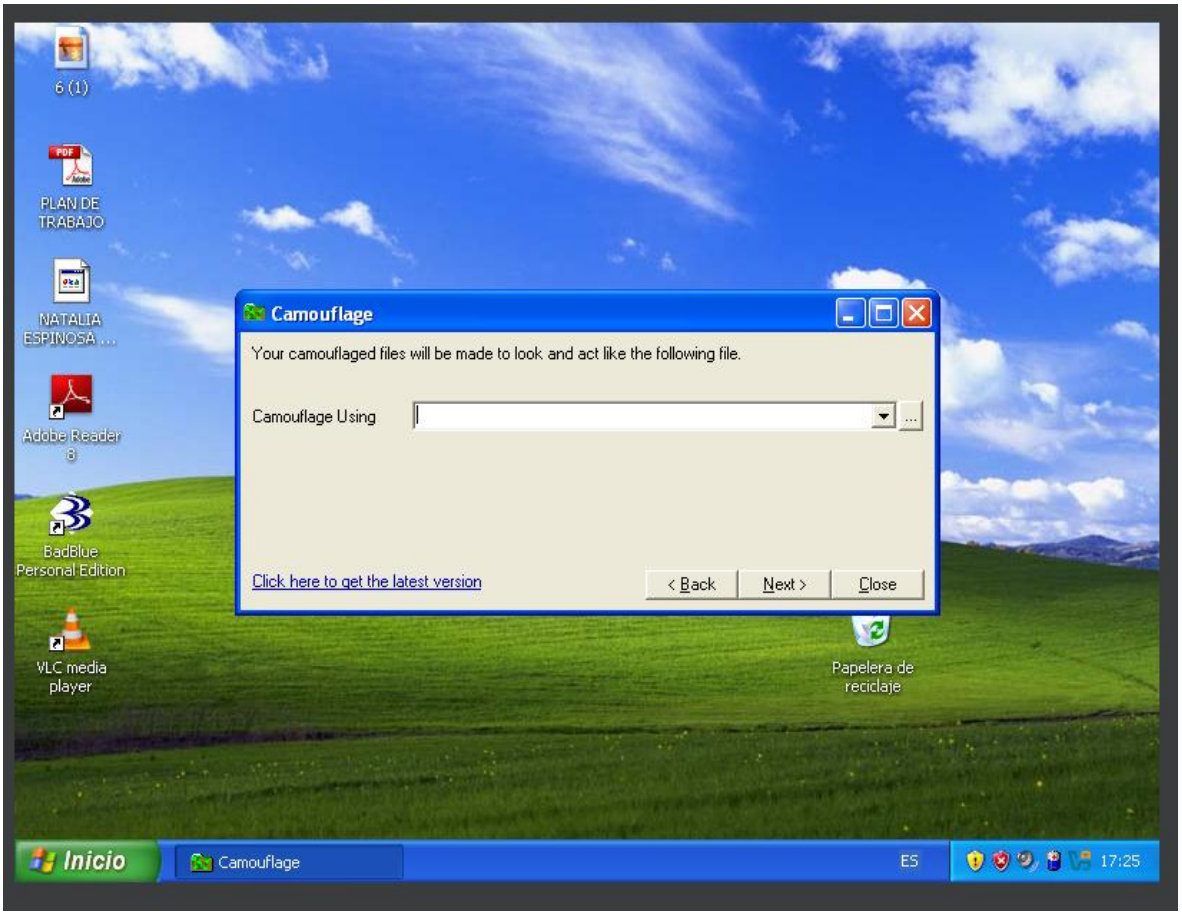


Ilustración 23 Selección de archivo de camuflaje

En este paso, el asistente mostró el campo **Camouflage Using**, desde el cual se debía seleccionar el archivo portador que contendría los documentos a camuflar. El sistema permitió buscar dicho archivo mediante el icono que cuenta con los tres puntos.

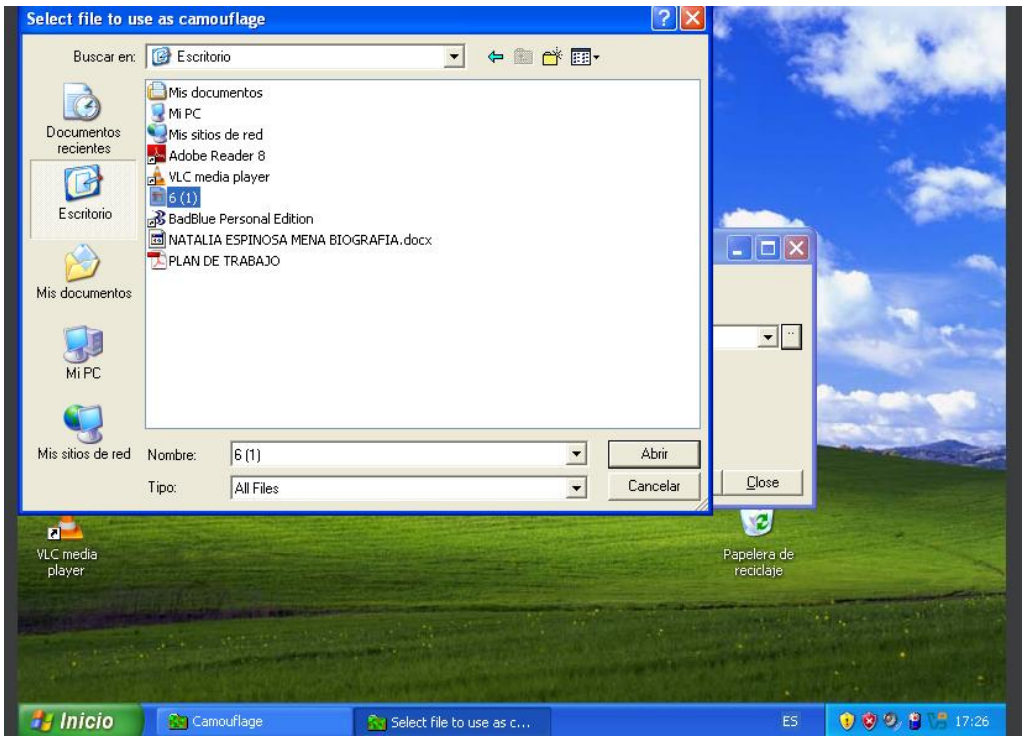


Ilustración 24 Explorador de archivos

Al seleccionar la opción para elegir el archivo portador, se abrió la siguiente ventana del explorador de archivos de Windows XP. Desde esta interfaz, el programa Camouflage permitió buscar y seleccionar el archivo que se utilizaría como contenedor para ocultar los documentos.

En este caso, se accedió a la ubicación Escritorio, donde se visualizaron los archivos disponibles, y la imagen que fue seleccionada como archivo portador.

Una vez identificado el archivo correspondiente, se hizo clic en el botón Abrir para confirmarlo y continuar con el proceso de camuflaje.

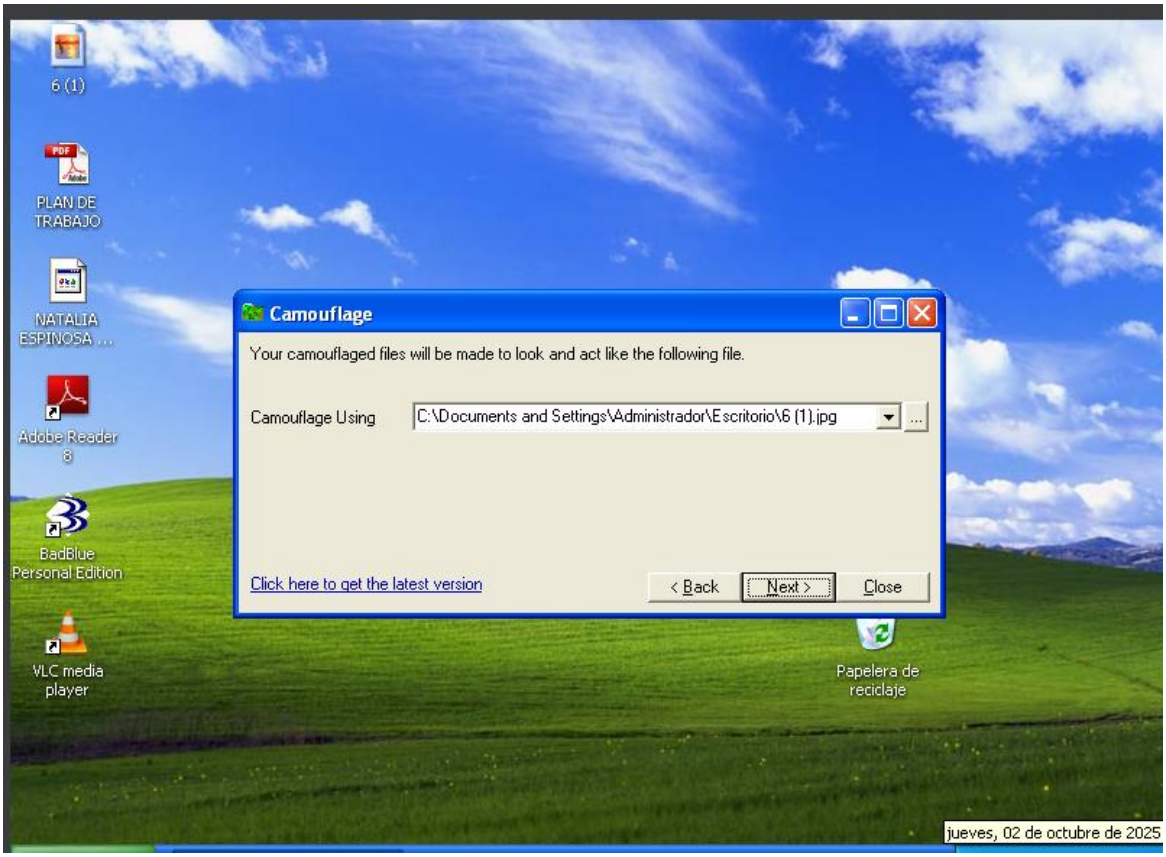


Ilustración 25 Ruta del archivo de camuflaje

Una vez seleccionado el archivo portador, el asistente de Camouflage mostró nuevamente la ventana principal con la ruta completa del archivo elegido, tal como se observa en la imagen.

En este caso, el programa indicó la dirección: C:\Documents and Settings\Administrador\Escritorio\6 (1).jpg, correspondiente a la imagen que serviría como contenedor para los archivos ocultos.

Tras confirmar la selección, se hizo clic en el botón Next para avanzar al siguiente paso del asistente.

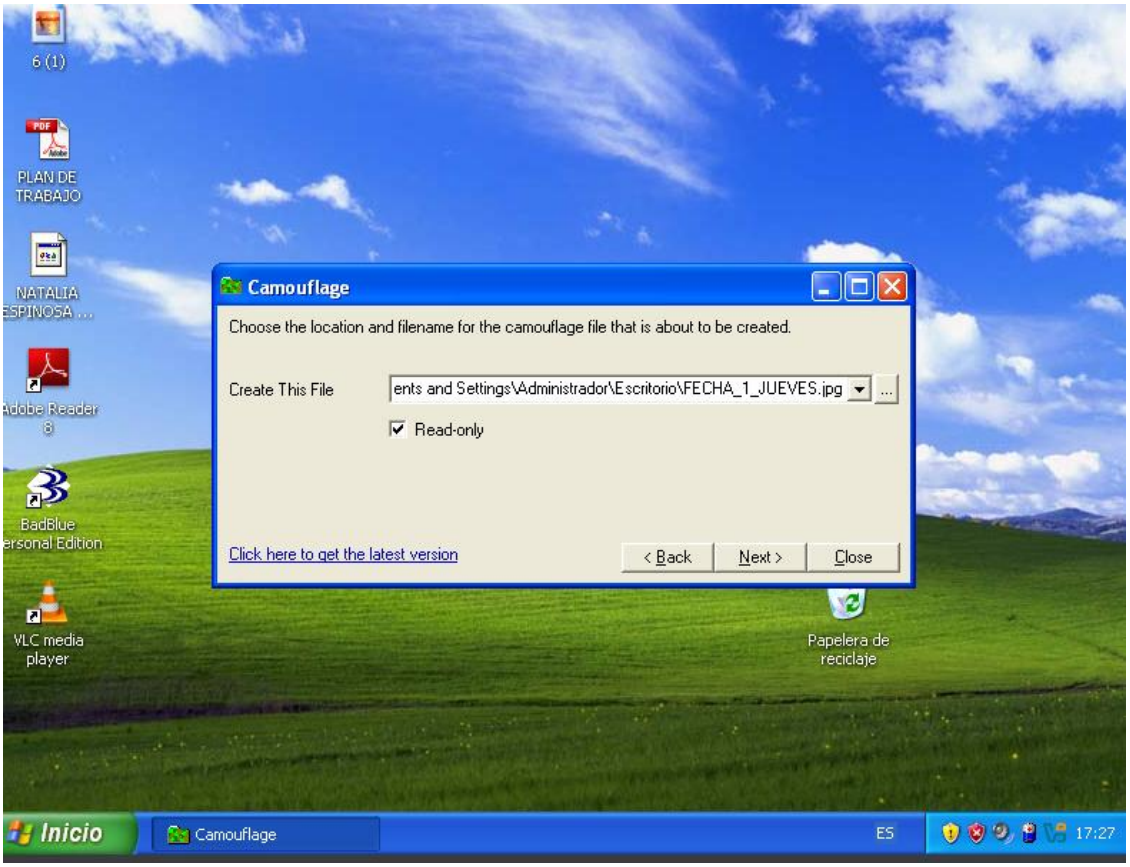


Ilustración 26 Cambio de Nombre al portador

En esta ventana, el programa Camouflage solicitó asignar un nuevo nombre al archivo portador que se generaría al finalizar el proceso de camuflaje. Por defecto, el sistema propuso la misma ruta del escritorio del usuario administrador.

En este caso, se cambió el nombre del archivo portador a **FECHA_1_JUEVES**.jpg luego, se hizo clic en el botón Next para continuar.

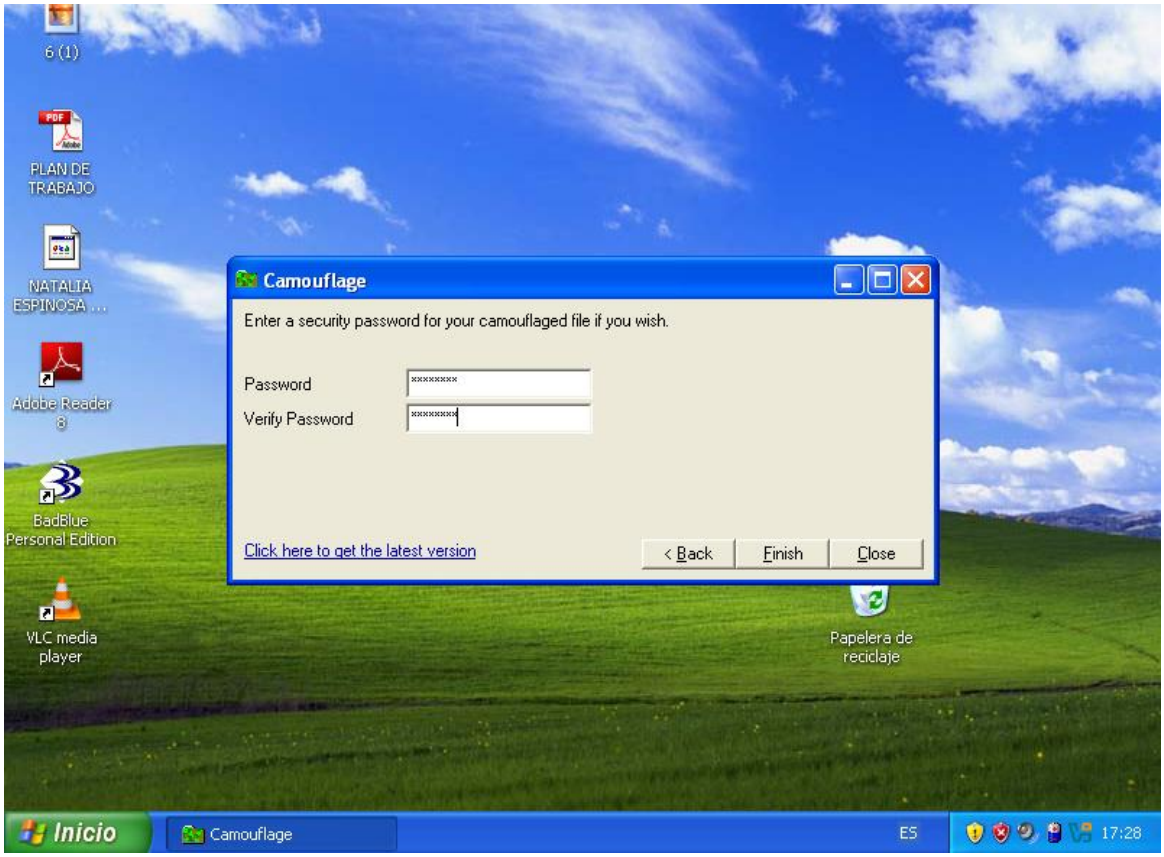


Ilustración 27 Contraseña Camouflage

En esta ventana, el asistente de Camouflage solicitó establecer una contraseña de seguridad para proteger el archivo camuflado que se iba a crear. Para ello, se ingresó la clave en el campo Password y se repitió en el campo Verify Password con el fin de confirmar su coincidencia. Una vez ingresados ambos valores correctamente, se hizo clic en el botón Finish para finalizar el proceso.

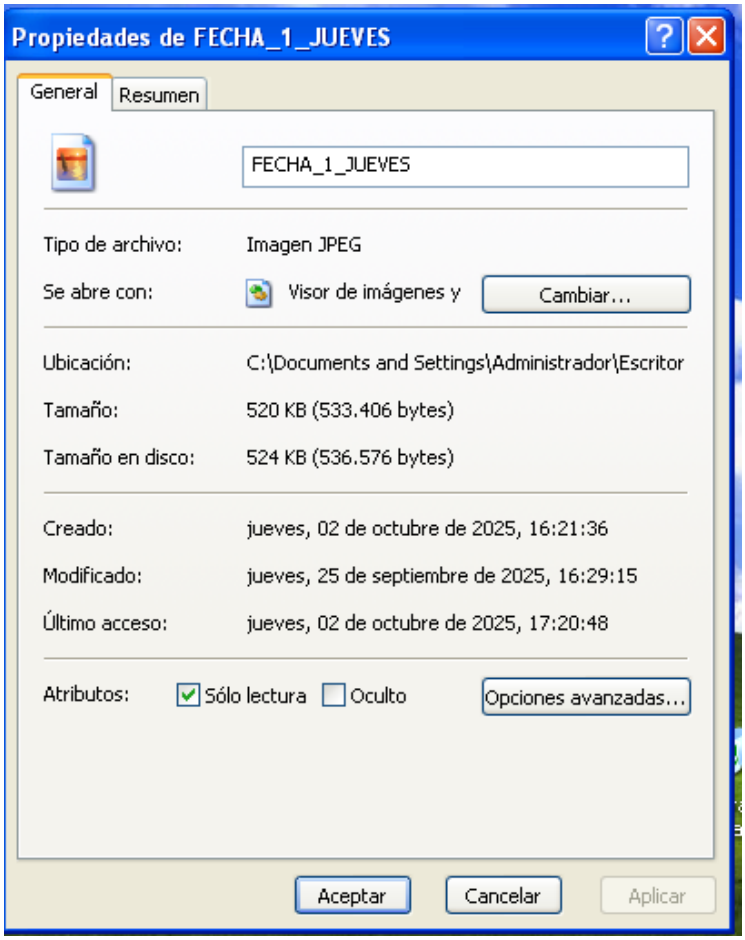


Ilustración 28 Imagen Portadora

Posteriormente, se localizó la imagen generada con el nuevo nombre en la ruta establecida. Al verificar sus propiedades, se observó un incremento en el tamaño del archivo, pasando de **157 KB (Ver imagen)** en su estado original a **520 KB** después del proceso de camuflaje.

Este cambio evidenció que los documentos seleccionados fueron correctamente ocultados dentro de la imagen portadora, confirmando que la herramienta Camouflage realizó el proceso de ocultamiento de manera exitosa.

1.1 ¿CUÁNTOS ARCHIVOS SE PUEDEN CAMUFLAR?

Para dar prueba de esto, se compartieron cierta cantidad de archivos: .exe, .pdf. .docx, .jpg. A continuación, se detalla los pasos:

En primer lugar, se compartieron los archivos desde el host hacia la máquina virtual Windows XP, organizándolos dentro de carpetas específicas. Estas carpetas se utilizaron para mantener separados los archivos por tipo y facilitar su selección durante las pruebas, tal como se muestra en la siguiente imagen.

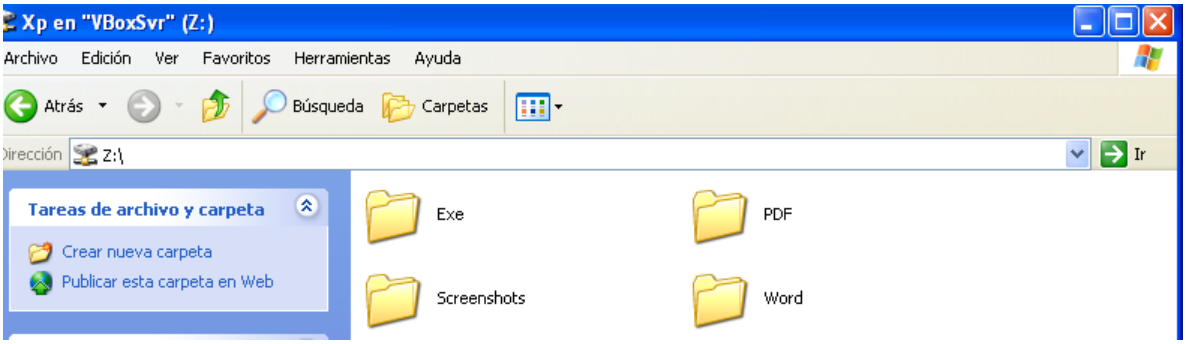


Ilustración 29 Carpetas de archivos compartidos

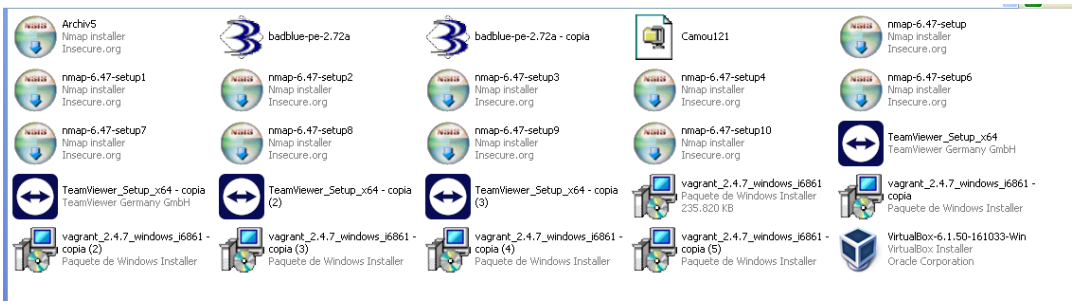


Ilustración 30 Archivos .exe

Estos fueron los archivos compartidos desde el equipo anfitrión hacia la máquina virtual con Windows XP, con el propósito de realizar las pruebas de capacidad de la herramienta Camouflage.

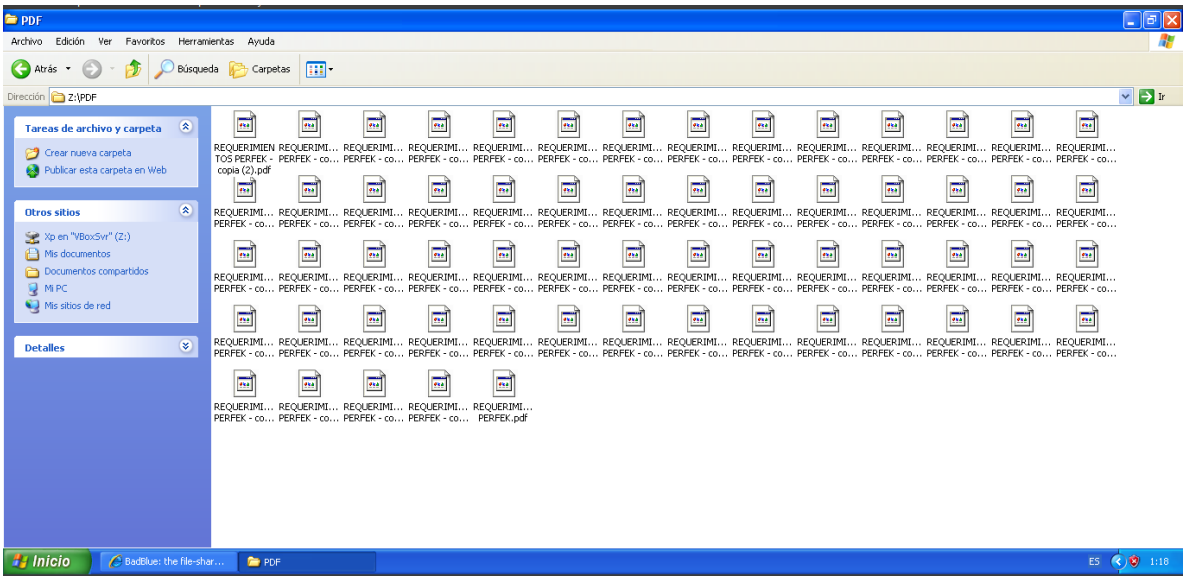


Ilustración 31 Archivos .pdf

Como se aprecia en las imágenes, los archivos incluían instaladores ejecutables (.exe), documentos (.docx), archivos PDF (.pdf) e imágenes (.jpg) Estos con el fin de evaluar el comportamiento de la herramienta al momento de ocultar diferentes tipos de archivos dentro de un portador.

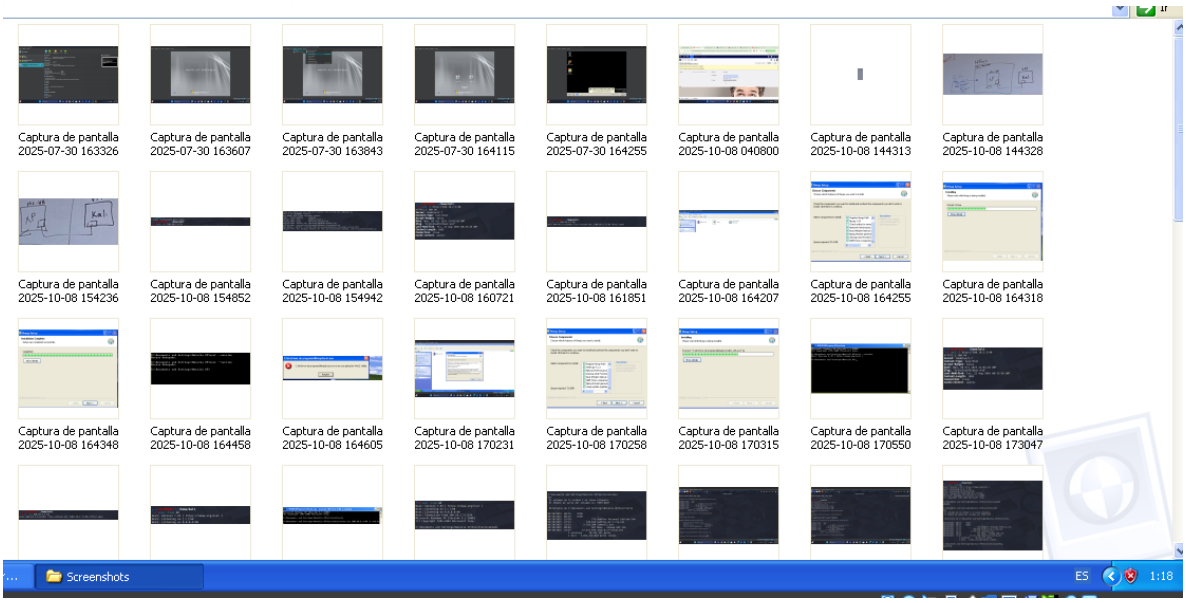


Ilustración 32 Archivos .jpg

En estas capturas, se observan los archivos jpg y los archivos .docx

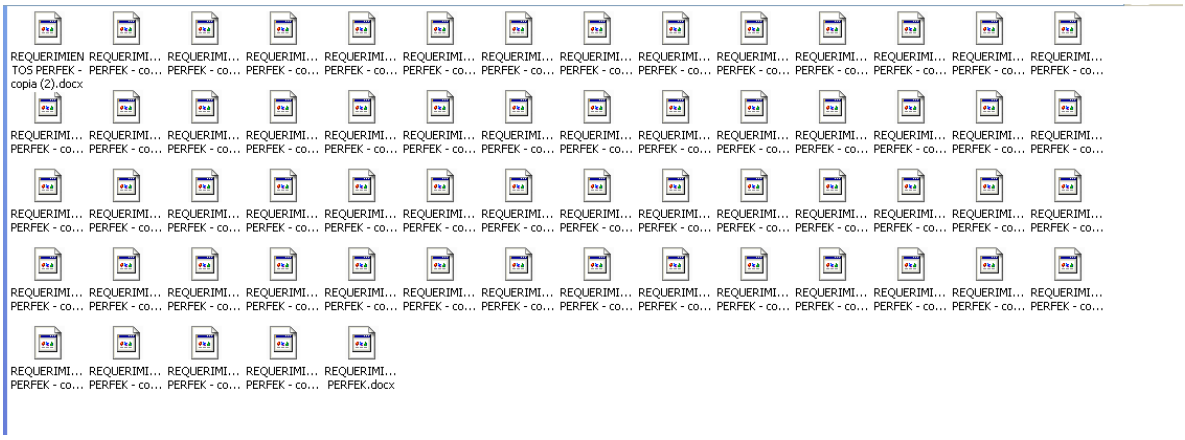


Ilustración 33 Archivos .docx

Una vez se dispusieron los archivos de prueba, se procedió a realizar el proceso de camuflaje utilizando la herramienta **Camouflage,** los pasos siguieron tal cual los mencionados

anteriormente. Los resultados obtenidos permitieron analizar el comportamiento del programa frente a distintos tipos y tamaños de archivos.

Se determinó que Camouflage no presenta un límite específico en cuanto a la cantidad de archivos que pueden ocultarse, sino que sus restricciones dependen principalmente del tamaño total de los datos a camuflar y del tipo de archivo portador seleccionado.

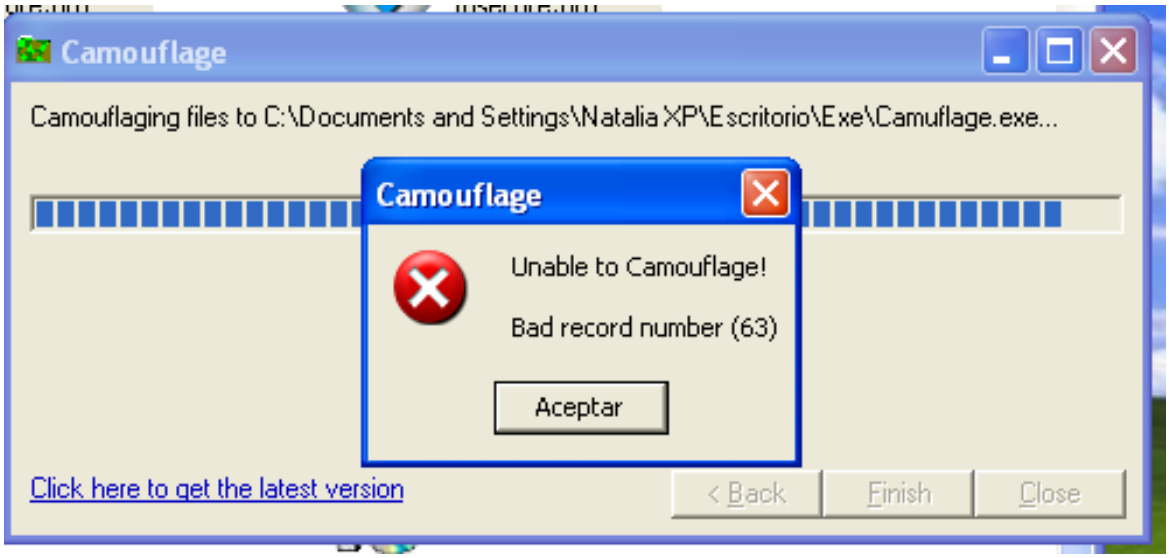
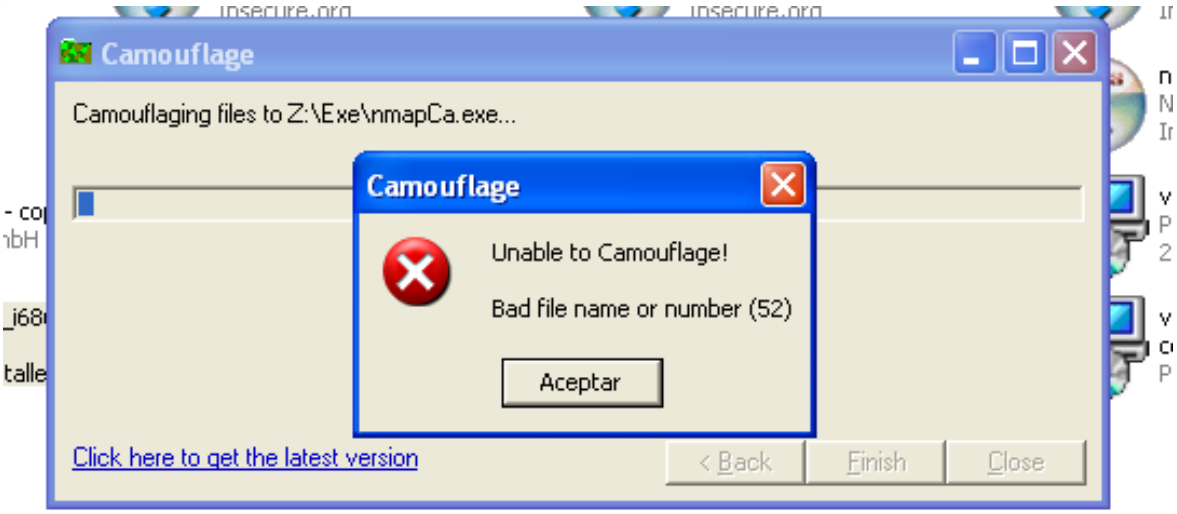


Ilustración 34 Error al camuflar

Durante las pruebas, se observó que al utilizar imágenes (.jpg) como archivos portadores, el programa permitió superar el tamaño original del archivo sin generar errores. Sin embargo, en el caso de los archivos ejecutables (.exe) y documentos PDF (.pdf), el sistema mostró fallos al intentar sobrepasar la capacidad del portador, impidiendo completar el proceso de camuflaje.

Las imágenes muestran los resultados obtenidos y los mensajes de error presentados durante las pruebas de límite realizadas con diferentes tipos de archivos.



Con base en las pruebas realizadas y en la documentación consultada, se determinó que Camouflage presenta un límite de capacidad variable, el cual depende del tipo de archivo portador y del sistema de archivos utilizado. En términos generales, la herramienta puede manejar un rango aproximado de entre 100 a 200 MB en la mayoría de los casos, aunque en condiciones específicas y con portadores de gran tamaño puede alcanzar hasta 4 GB.

2 CAPÍTULO 2: BADBLUE

En este capítulo se considera necesario realizar la conexión a XP por BadBlue en el puerto hhtp 80, para ello, a continuación, se detallan los pasos seguidos:

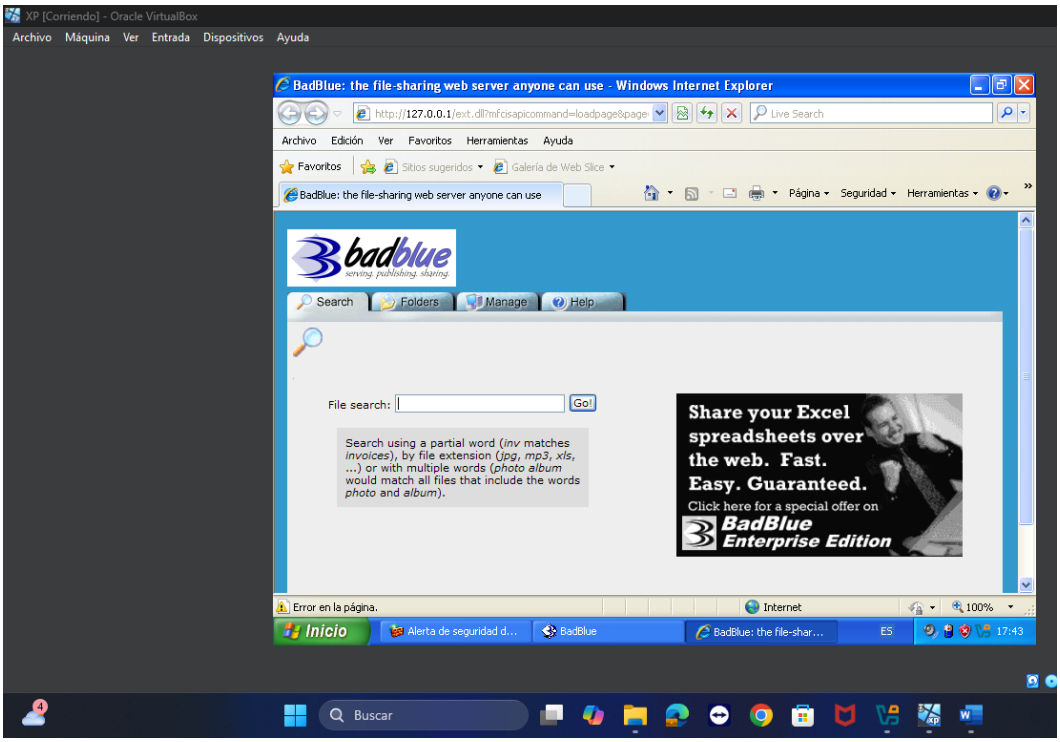


Ilustración 35 Página principal BadBlue

En la imagen se muestra la página principal del servicio BadBlue ejecutándose en el sistema operativo Windows XP. Se accedió a su interfaz web a través del navegador Internet Explorer, utilizando la dirección **http://127.0.0.1/** correspondiente al localhost de la máquina.

El siguiente paso consistió en realizar un escaneo del segmento de red:

Ilustración 36 Escaneo de red

Se inició la máquina Kali Linux y, tras obtener privilegios de super usuario con **sudo su**, se ejecutó el escaneo de la red con nmap para identificar hosts y servicios activos. Con el comando **nmap -sV 100.10.2.0/24.**

Muestra el resultado el puerto de BadBlue abierto: Entre los resultados del escaneo realizado con nmap, se identificó que la máquina con dirección **IP 100.10.2.5** tenía varios puertos TCP abiertos. Entre ellos, destacó el puerto **80**, asociado al servicio HTTP donde se ejecutaba BadBlue httpd 2.7

```
Nmap scan report for pool-100-10-2-5.prvdri.fios.verizon.net (100.10.2.5)
Host is up (0.00080s latency).
Not shown: 996 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
MAC Address: 08:00:27:C7:64:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Ilustración 37 Puerto BadBlue

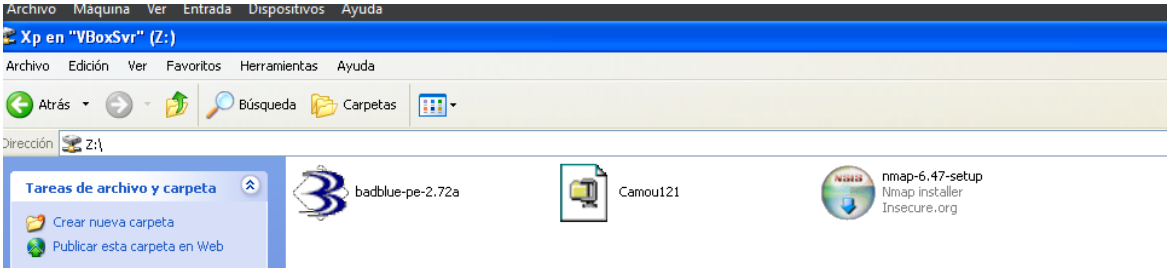


Ilustración 38 Nmap.exe (Netcat)

Para la conexión por el puerto 80, en investigaciones se encontró la herramienta netcat cuyo propósito general es abrir conexiones, la cual se usó posteriormente, siguiendo los siguientes pasos:

Desde la página oficial se descargó la versión compatible con Windows xp, ya que en Kali ya viene integrado: Una vez descargado en el equipo Host se compartió a través de la carpeta compartida en XP, como se observa en la imagen anterior.

Se siguieron los pasos del instalador hasta completar la instalación como se muestra en la siguiente secuencia de imágenes:

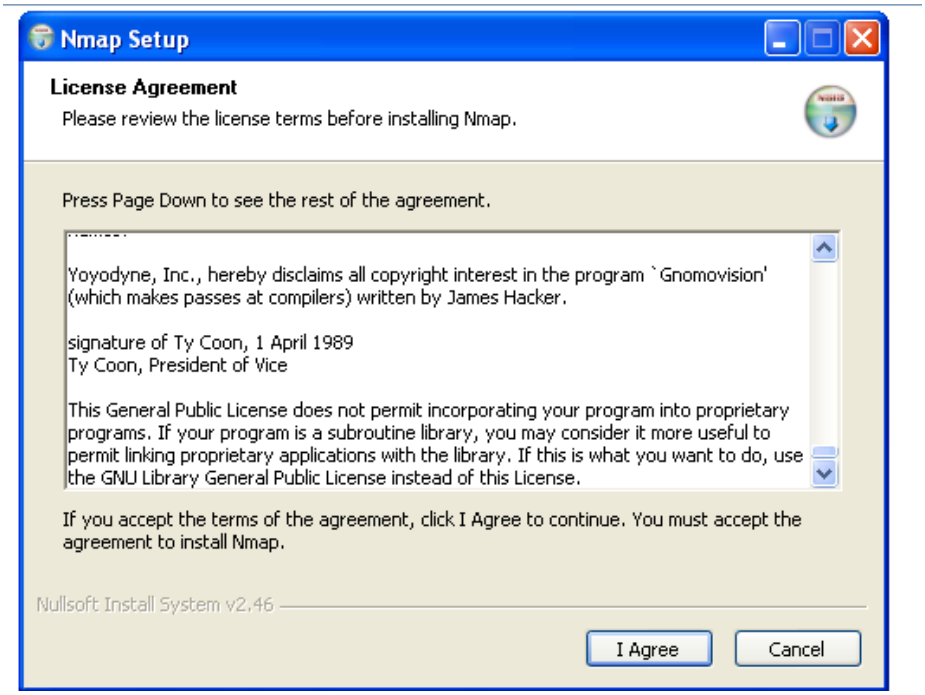


Ilustración 39 Acuerdo de licencia Ncat

Al iniciar el instalador de Nmap en la máquina Windows XP, se presentó primeramente la ventana del acuerdo de licencia correspondiente al asistente de instalación. En dicha ventana se solicitó revisar los términos de la licencia y, para continuar con la instalación, se seleccionó la opción **I Agree.**

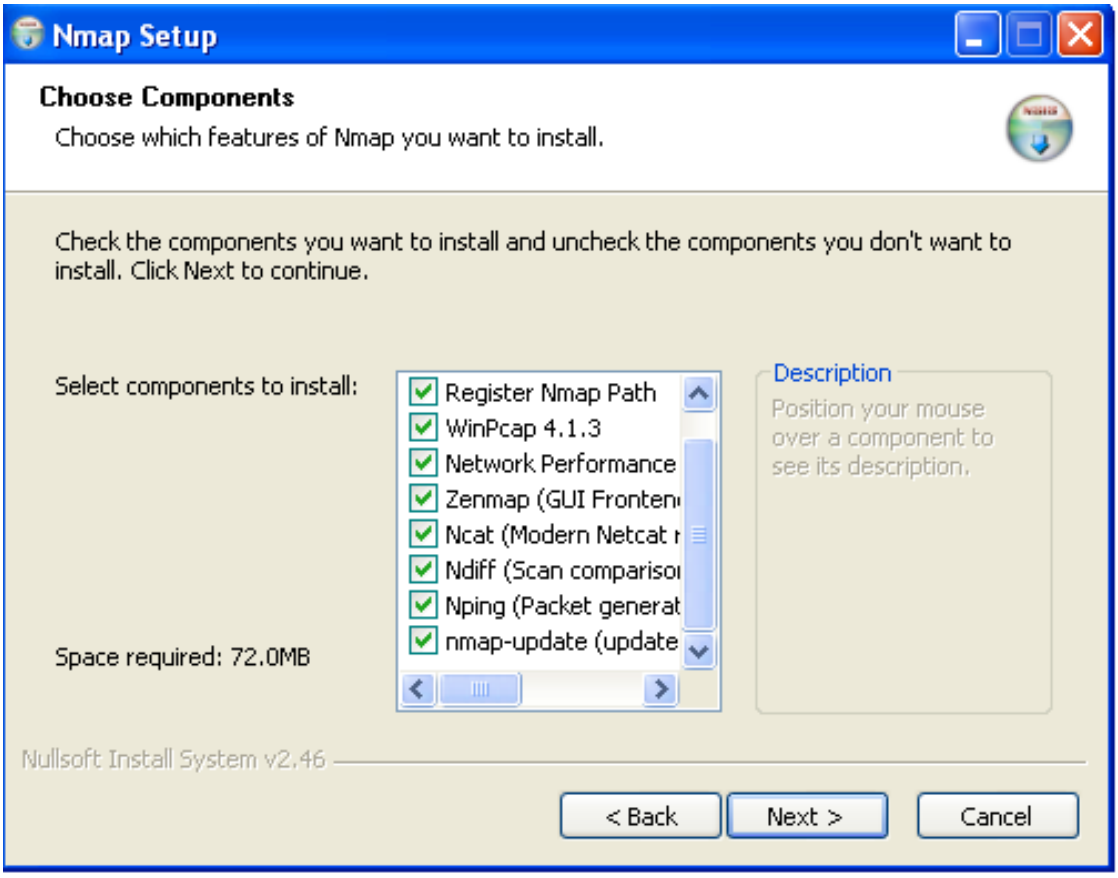


Ilustración 40 Instalación Netcat

La siguiente ventana mostro la selección de componentes adicionales donde, se verifico que Netcat (Ncat) estuviera seleccionado dentro de los componentes de instalación. Una vez confirmadas las opciones, se hizo clic en **Next** para continuar con el proceso de instalación.

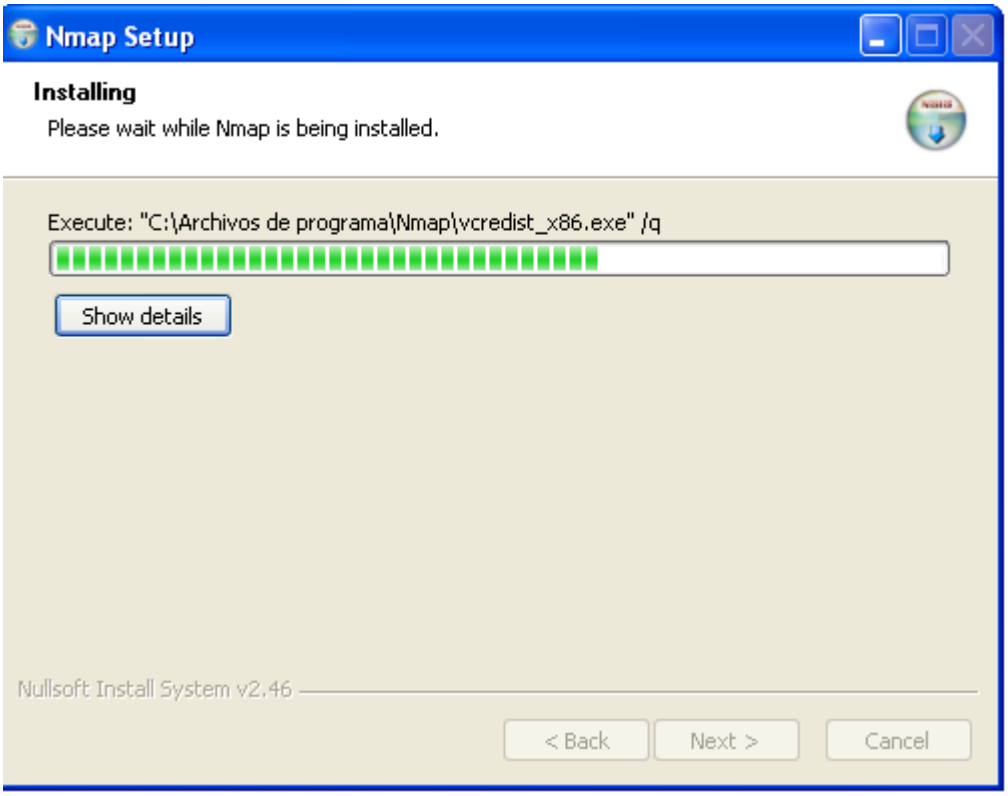


Ilustración 41 Proceso de finalización de instalación Netcat

El asistente mostró la ventana de progreso de instalación de Nmap, donde se pudo observar la barra de avance que indicaba la copia e instalación de los componentes seleccionados, se esperó hasta que la barra de progreso alcanzó el 100 %, momento en el cual se completó la instalación.

Ilustración 42 Visualización en el Escritorio de Nmap

Se procedió a verificar la correcta instalación del componente Ncat desde la consola de comandos de Windows XP. Para ello, se ejecutó la instrucción:

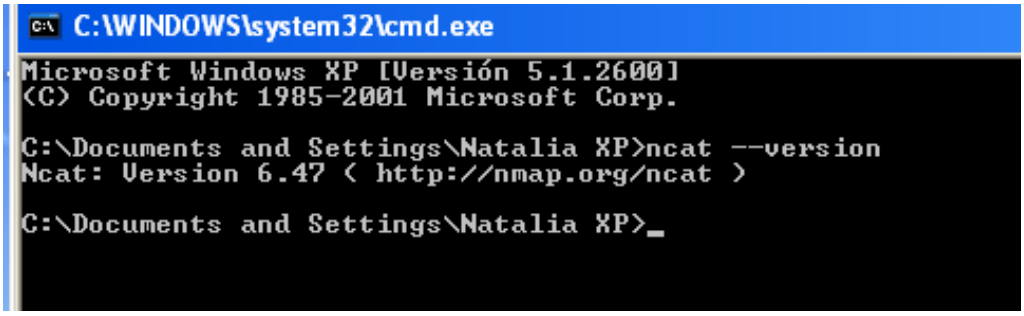


Ilustración 43 Verificación de la versión Netcat

En la máquina Kali Linux también se verificó la presencia de la herramienta Netcat (Ncat) ejecutando el comando: **ncat –versión**

El sistema indicó que el programa no se encontraba instalado, por lo que se procedió a instalarlo.

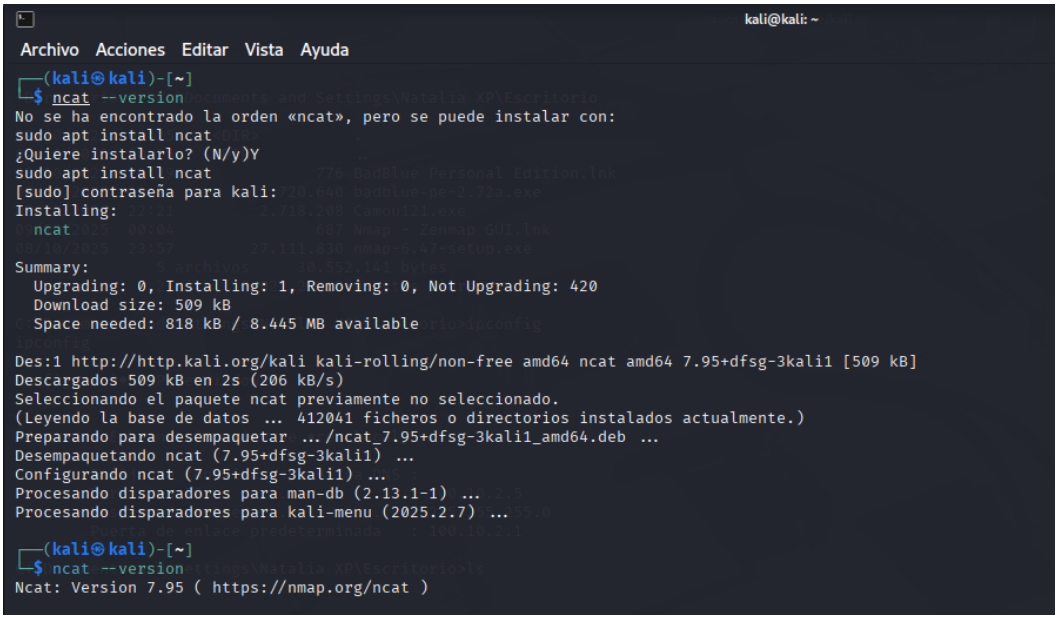


Ilustración 44Instalacion Netcat Kali

Una vez finalizada la instalación, se volvió a ejecutar el comando de verificación y se confirmó que la herramienta había sido instalada correctamente.

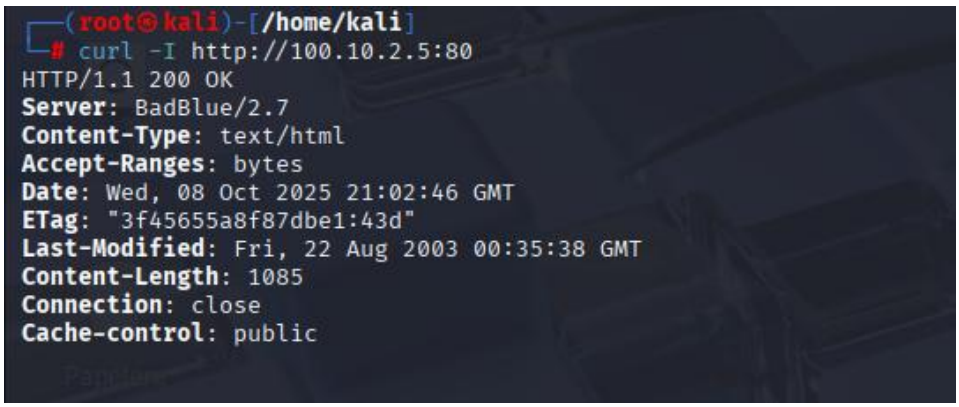


Ilustración 45 Comprobación que el servicio web responde

En la imagen anterior se muestra la comprobación de respuesta del servicio web BadBlue mediante el comando: curl -I http://100.10.2.5:80

La respuesta del servidor fue HTTP/1.1 200 OK, lo que confirmó que el servicio web se encontraba activo y operativo en la dirección IP 100.10.2.5 a través del puerto 80.

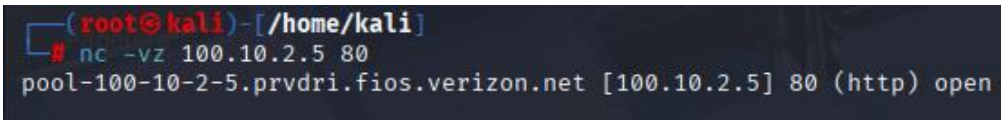


Ilustración 46Comprobación puerto TCP

También se realizó la verificación del estado del puerto 80 utilizando la herramienta Netcat (nc) desde la máquina Kali Linux. El comando ejecutado fue: nc -vz 100.10.2.5 80

El resultado obtenido indicó que el puerto 80 (HTTP) en la dirección 100.10.2.5 se encontraba abierto, mostrando el mensaje open, como se observa en la imagen.

Una vez realizadas las comprobaciones, el paso siguiente consistió en poner la maquina en escucha para recibir conexiones entrantes:

Ilustración 47 máquina a la escucha

La máquina Kali Linux fue configurada en modo escucha utilizando la herramienta Ncat. Para ello, se ejecutó el comando: **ncat -lvnp 80**

Con esta instrucción, el sistema inició el proceso de escucha en el puerto 80, quedando a la espera de conexiones entrantes provenientes de otros equipos de la red.

La salida del comando mostró la versión 7.95 de Ncat y los mensajes Listening on [::]:80 y Listening on 0.0.0.0:80, lo que indicó que la máquina estaba escuchando correctamente.

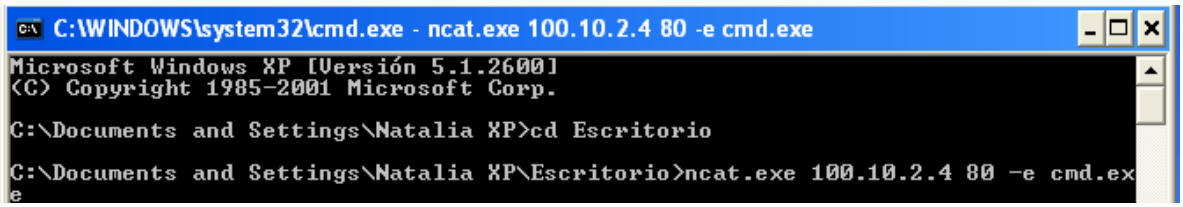


Ilustración 48 conexión TCP

Desde la máquina Windows XP también se ejecutó la conexión hacia Kali Linux utilizando la herramienta Ncat.

Primero, se accedió al directorio donde se encontraba el archivo ejecutable y luego se ejecutó el siguiente comando en la consola de cmd.exe: ncat.exe 100.10.2.4 80 -e cmd.exe

Con ese comando, la máquina Windows XP abrió una conexión hacia la dirección 100.10.2.4 (Kali Linux) usando el puerto 80 y envió la consola de comandos (cmd.exe) a través de esa conexión.

De esta manera, la ventana de comandos de Windows quedó conectada a la máquina Kali, lo que permitió intercambiar órdenes y respuestas de forma remota entre ambos equipos.

En Kali Linux, el puerto en escucha acepto la conexión y se abrió una consola remota de Windows: La máquina Kali Linux recibió la conexión proveniente de Windows XP a través del puerto 80.

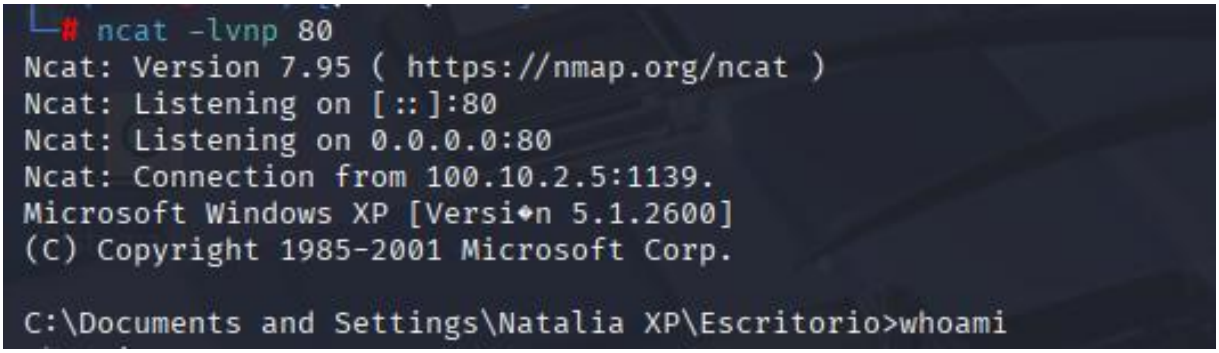


Ilustración 49 Conexión aceptada

Ncat mostró el mensaje Connection from 100.10.2.5, indicando que la máquina con esa dirección IP, correspondiente a Windows XP, logró conectarse con éxito.

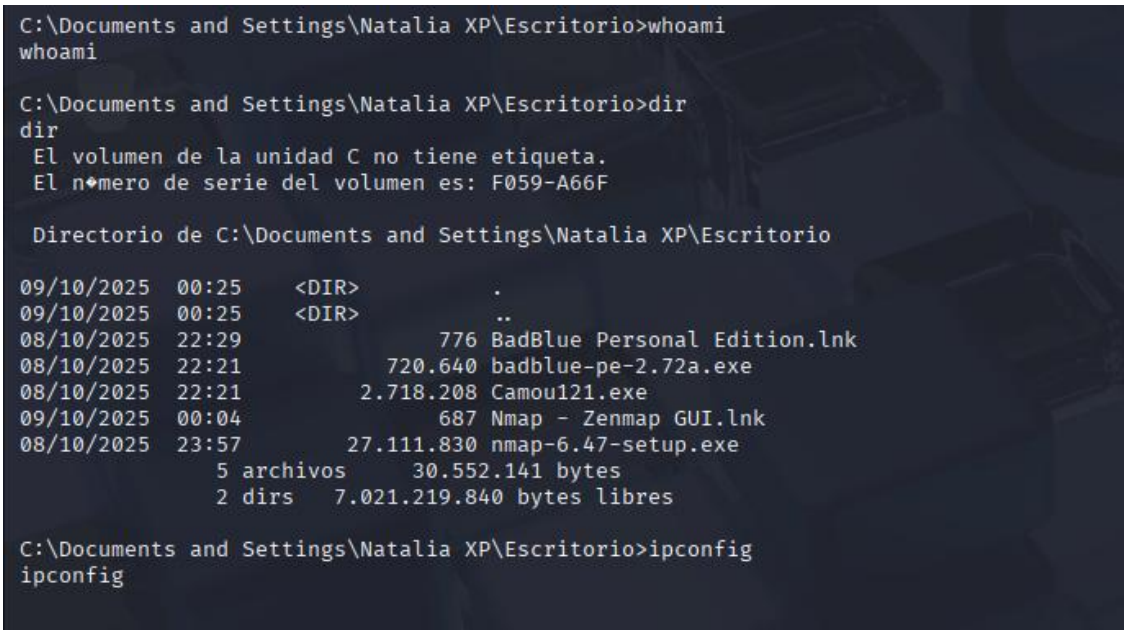


Ilustración 50 Listado del directorio

Se ejecutaron varios comandos para comprobar el acceso y la correcta comunicación. Primero, se utilizó el comando whoami, el cual mostró el nombre del usuario activo en la máquina XP.

Luego se ejecutó el comando dir, que permitió listar el contenido del escritorio de Windows XP. En la salida se observaron varios archivos, como BadBlue Personal Edition, Camouflage, Nmap – Zenmap GUI, y nmap-6.47-setup.exe y por último el comando ipconfig para visualizar la configuración de red y comprobar la dirección IP asignada a la máquina XP.

3 RECOMENDACIONES

Se recomienda que las máquinas virtuales se configuren en la misma red NAT para asegurar una comunicación estable entre Kali Linux y Windows XP. También, utilizar la versión correcta de Netcat compatible con Windows XP para evitar problemas de compatibilidad.

4 CONCLUSIONES

Camouflage se presenta como una herramienta eficaz para el ocultamiento de archivos, lo que pone en evidencia la necesidad de implementar medidas de seguridad que permitan detectar y prevenir este tipo de técnicas, se resalta la importancia de verificar los tamaños de los archivos para identificar datos sospechosos que puedan indicar la presencia de datos ocultos.

Por otra parte, se logró establecer correctamente la conexión a través del puerto 80 utilizando la herramienta de red Netcat (Ncat), lo que permitió una comunicación efectiva entre las máquinas virtuales y una mejor comprensión del funcionamiento de los servicios de red.

En general, el laboratorio se desarrolló con éxito, contribuyendo al fortalecimiento de los conocimientos en seguridad de redes, y brindando una experiencia práctica sobre el uso y análisis de herramientas relacionadas con la administración y la protección de sistemas.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

5 BIBLIOGRAFÍA

Ellingwood, J. (5 de Agosto de 2025). *Tutorials.DigitalOcean*. Obtenido de DigitalOcean: https://www.digitalocean.com/community/tutorials/how-to-use-netcat-to-establish-and-test-tcp-and-udp-connections

Morales, R. S. (25). INFORME LABORATORIO CAMUOFLAGE Y BADBLUE. Quibdó, Colombia: Universidad Tecnológica del Chocó Diego Luis Córdoba. Recuperado el 09 de 10 de 2025