INFORME #1 ANÁLISIS PRÁCTICO DE TÉCNICAS GENERACIÓN DE HASH FORENSE Y EXPLOTACIÓN DE VULNERABILIDADES EN ENTORNOS VIRTUALIZADOS CON KALI LINUX Y WINDOWS XP

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIÓNES E INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIÓN

INTRODUCCIÓN

La seguridad informática se ha convertido en uno de los pilares más importantes dentro del campo de las telecomunicaciones y las tecnologías de la información. En la actualidad, la protección de los sistemas, redes y datos personales requiere no solo conocimiento teórico, sino también la capacidad de **realizar pruebas prácticas y auditorías controladas** que permitan comprender cómo operan las amenazas en escenarios reales.
Este informe presenta un proceso experimental en el cual se implementan y analizan distintas herramientas y técnicas de **seguridad y auditoría en redes**, haciendo uso de entornos virtualizados con **Oracle VirtualBox**, **Kali Linux** y **Windows XP**. La metodología aplicada se centra en la instalación de controladores, la configuración de carpetas compartidas, la creación de archivos camuflados mediante **esteganografía con el programa Camouflage**, la generación de **hashes forenses** para verificar la integridad de datos, y finalmente, la **explotación controlada de una vulnerabilidad conocida en el servidor BadBlue 2.7**.

A través de estas actividades, el estudiante adquiere habilidades prácticas en **virtualización, análisis forense digital y pruebas de penetración (pentesting)**, comprendiendo el ciclo completo de una auditoría de seguridad desde la preparación del entorno hasta la identificación de brechas explotables. Además, se promueve el pensamiento crítico frente a la importancia de los principios de confidencialidad, integridad y disponibilidad de la información (CIA triad), fundamentales en la gestión moderna de la ciberseguridad. Este trabajo no solo busca reforzar los conocimientos técnicos, sino también generar conciencia sobre la **responsabilidad ética y profesional** en el uso de herramientas de hacking y auditoría, recordando que su correcta aplicación permite fortalecer la seguridad de los sistemas y prevenir incidentes de tipo cibernético en instituciones, empresas y redes personales.

OBJETIVOS

Objetivo general

Implementar y analizar herramientas de seguridad informática en entornos virtualizados mediante la utilización de Kali Linux y Windows XP, con el propósito de comprender las técnicas de esteganografía, generación de hash forense y explotación de vulnerabilidades en sistemas.

Objetivos específicos

Configurar y optimizar el entorno de trabajo en Oracle VirtualBox para realizar prácticas seguras de auditoría y pentesting.

Instalar y probar herramientas de **esteganografía (Camouflage)** para ocultar información dentro de archivos y evaluar su eficacia.

Generar y verificar **hashes forenses (SHA1)** en Kali Linux para garantizar la integridad y autenticidad de los datos digitales.

Ejecutar pruebas controladas de **explotación de vulnerabilidades** en el servicio BadBlue 2.7, comprendiendo su impacto en la seguridad de un sistema.

Documentar los resultados obtenidos y reflexionar sobre la aplicación ética de las herramientas empleadas en procesos de auditoría y ciberseguridad.

PLANTEAMIENTO DEL PROBLEMA

En el contexto actual, las organizaciones dependen en gran medida de sus sistemas informáticos para almacenar y procesar información crítica. Sin embargo, el crecimiento de las amenazas cibernéticas y las vulnerabilidades inherentes a los sistemas operativos hacen indispensable el desarrollo de competencias en **análisis, detección y mitigación de riesgos**

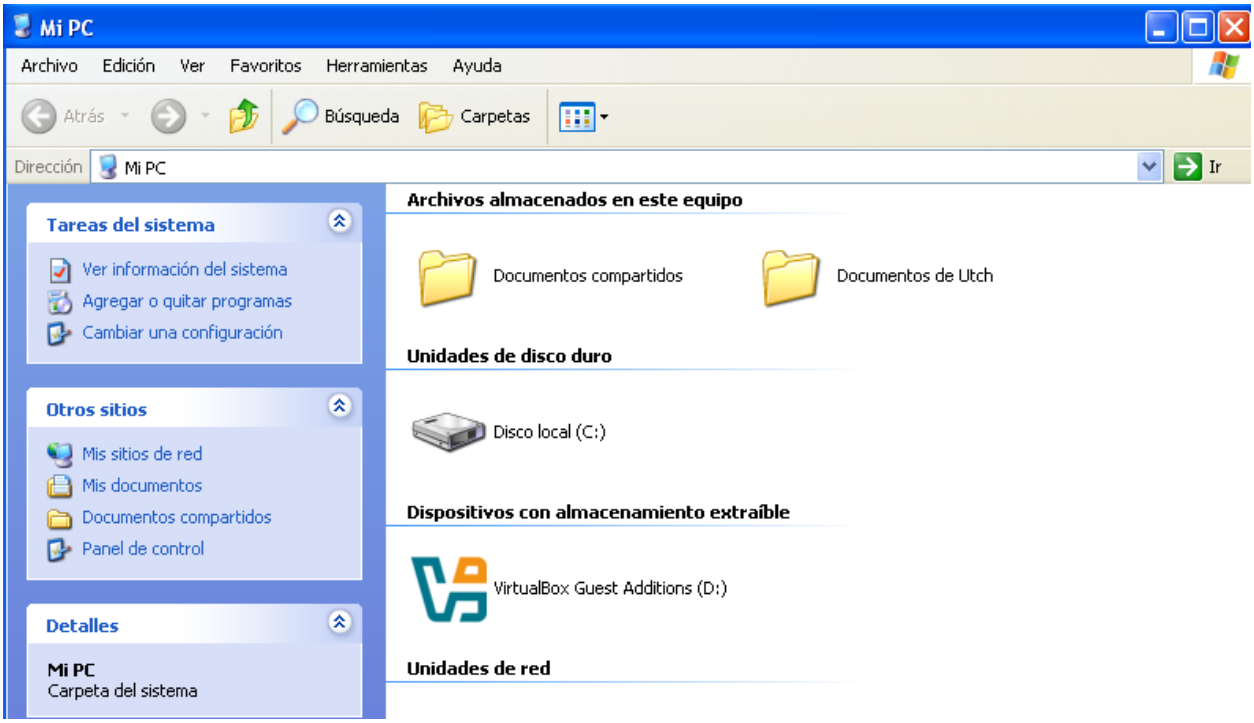
digitales.

Una de las principales dificultades que enfrentan los futuros ingenieros y auditores de redes es la **falta de experiencia práctica** en el uso de herramientas profesionales de ciberseguridad. A menudo, los estudiantes conocen la teoría, pero no disponen de entornos seguros donde puedan experimentar con técnicas de explotación, análisis forense o esteganografía sin comprometer equipos reales.

Por ello, surge la necesidad de **crear un laboratorio virtual controlado** en el que se simulen escenarios de ataque y defensa, utilizando tecnologías como **VirtualBox y Kali Linux**. En este contexto, el presente trabajo plantea el desafío de **implementar herramientas forenses y de auditoría** que permitan comprender los mecanismos de vulnerabilidad y las estrategias de protección aplicables en entornos reales, fortaleciendo así las capacidades técnicas y éticas de los futuros profesionales de la seguridad informática.

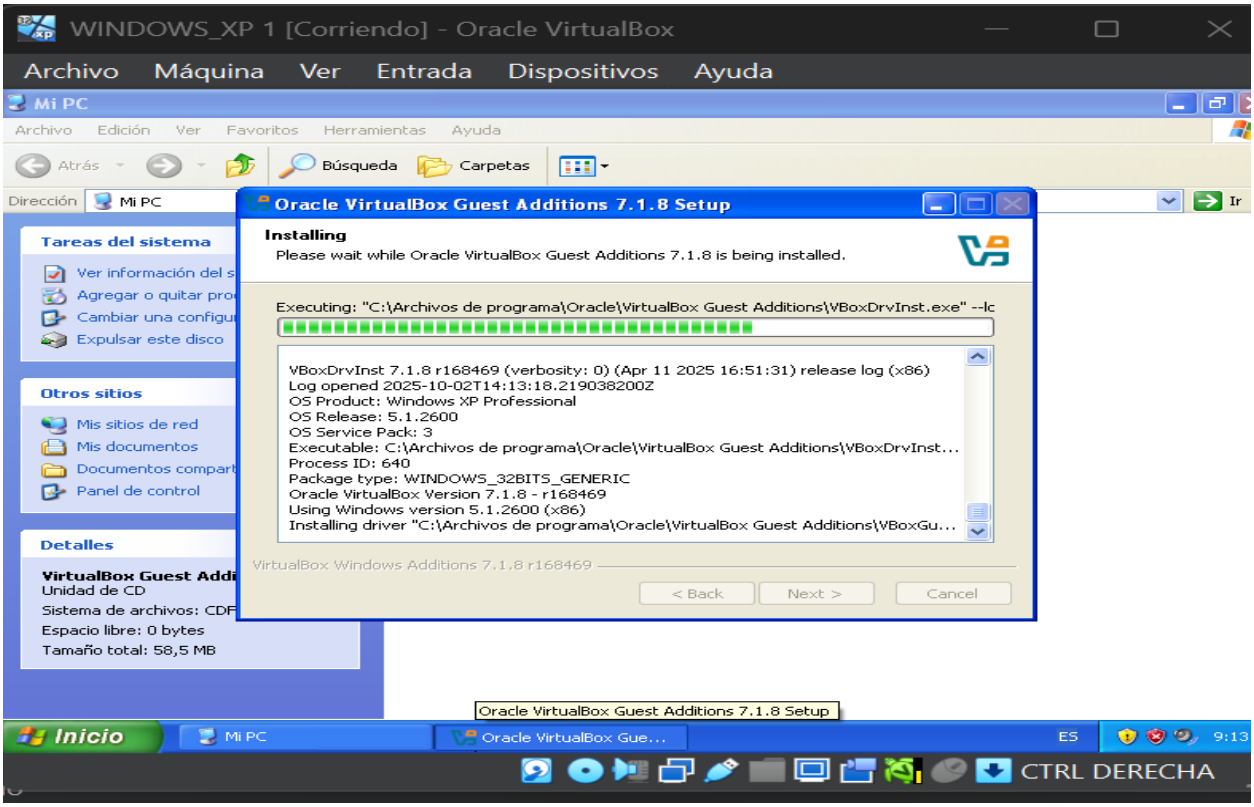
PRÁCTICA EN CLASES

Paso 1: En esta imagen se muestra el proceso de instalación de Oracle VirtualBox Guest Additions versión 7.1.8 dentro de una máquina virtual con Windows XP Professional Service Pack 3. Este complemento permite mejorar la integración entre el sistema anfitrión y el sistema virtual, optimizando funciones como la visualización, el uso compartido del portapapeles y la sincronización del cursor del ratón



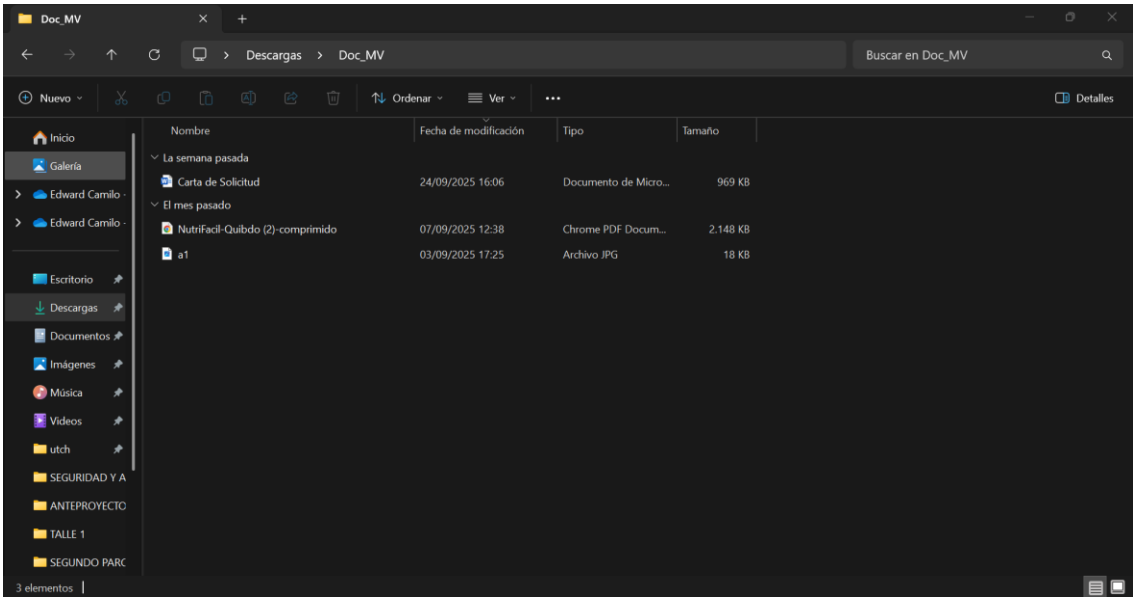
1 IOracle VirtualBox Guest Additions

Aquí se observa el contenido del explorador "Mi PC" en Windows XP, donde se muestra la unidad de disco **VirtualBox Guest Additions (D:)** montada correctamente. Esta acción indica que el instalador ha sido insertado de manera virtual y está listo para ejecutarse, paso previo a la instalación de los controladores y utilidades que mejoran el rendimiento de la máquina virtua



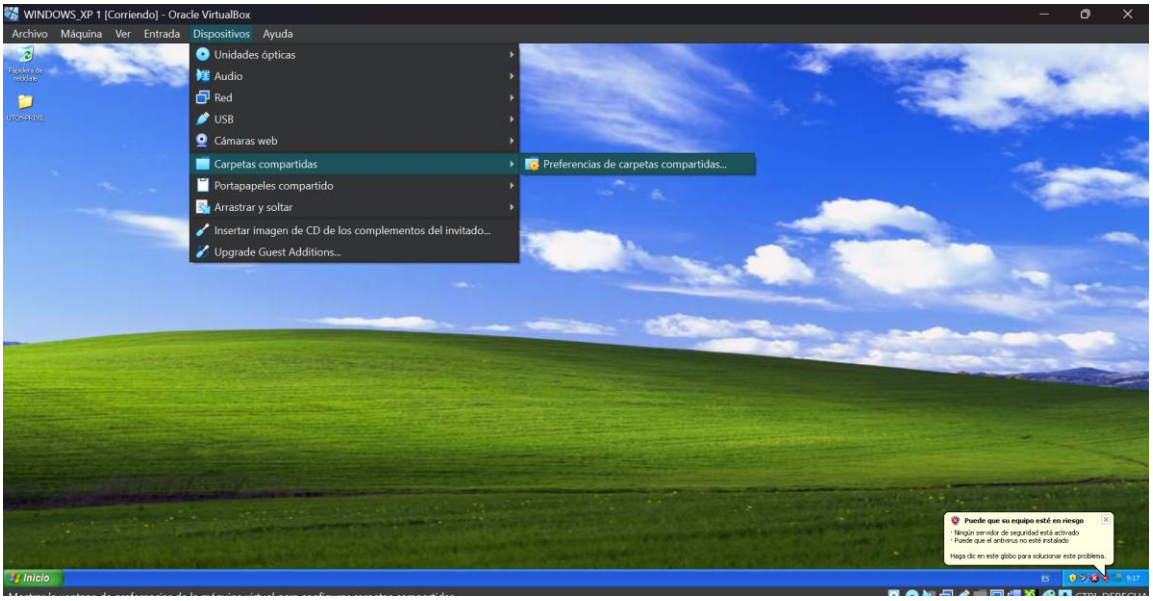
2 Instalación de Oracle VirtualBox Guest Additions

Paso 2: Se crean en el explorador de archivos de Windows 11 con la carpeta **Doc_MV**, que contiene varios documentos y archivos de trabajo. Esta carpeta será utilizada como carpeta compartida entre el sistema anfitrión y la máquina virtual, permitiendo el intercambio de información sin necesidad de dispositivos externos.

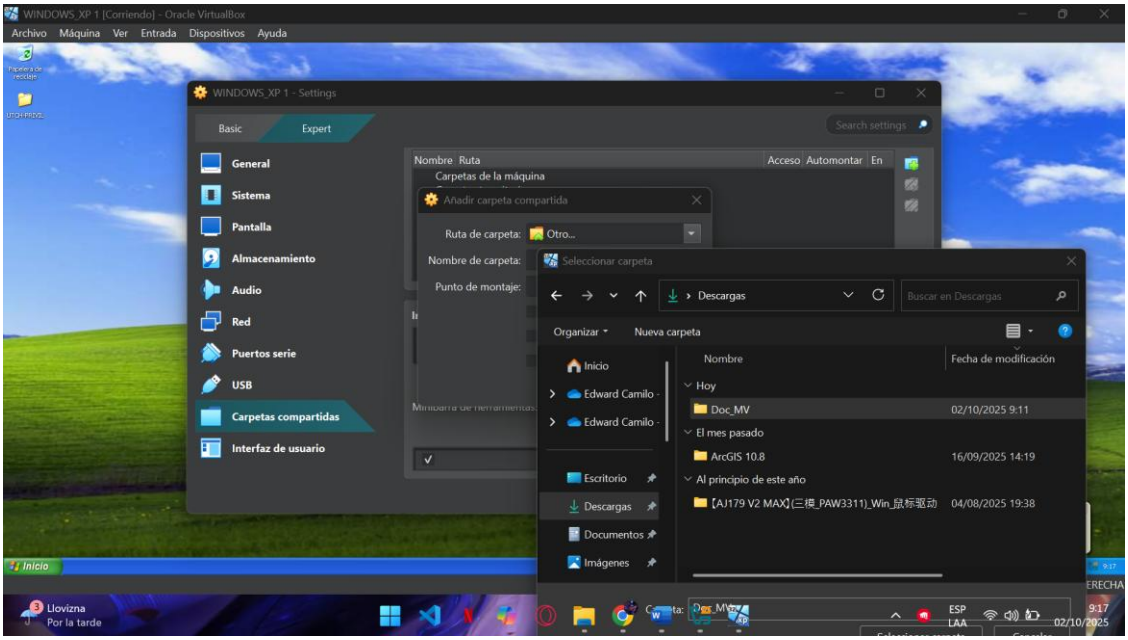


3. Exploración de la carpeta Doc_MV en el sistema anfitrión

En esta captura se observa la interfaz de VirtualBox con la máquina virtual de Windows XP en ejecución. Desde el menú Dispositivos > Carpetas compartidas > Preferencias de carpetas compartidas, se accede a la configuración donde se pueden añadir, modificar o eliminar carpetas compartidas entre ambos sistemas.

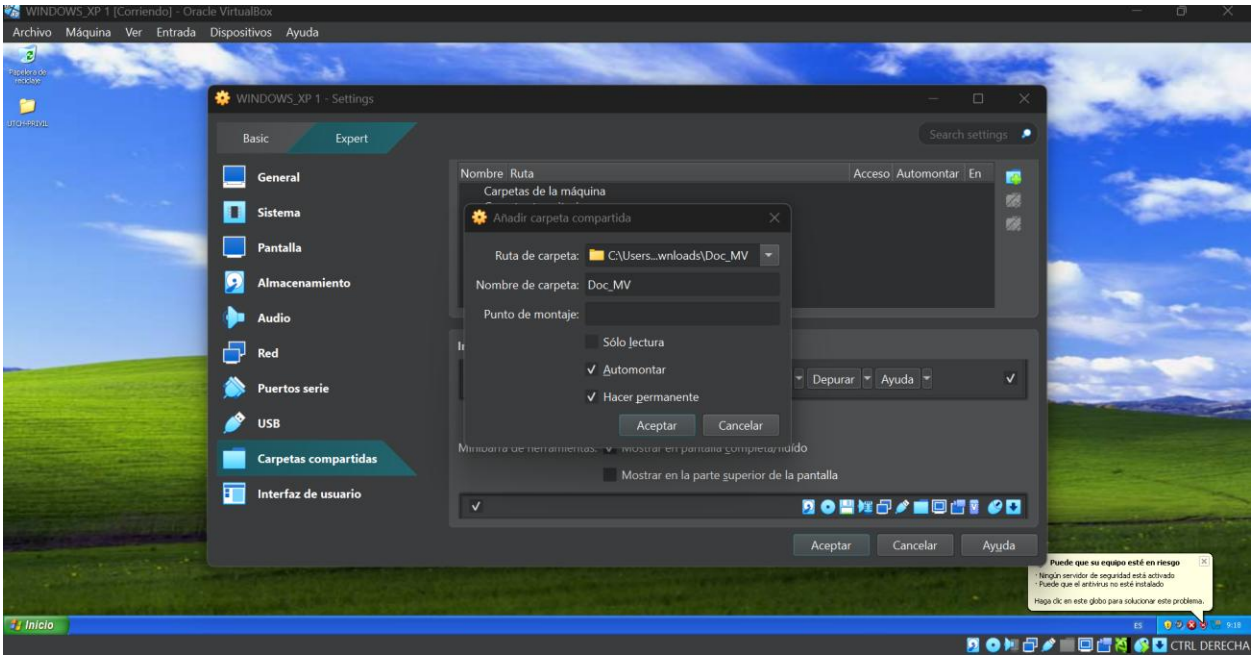


4. Acceso a las preferencias de carpetas compartidas en VirtualBox



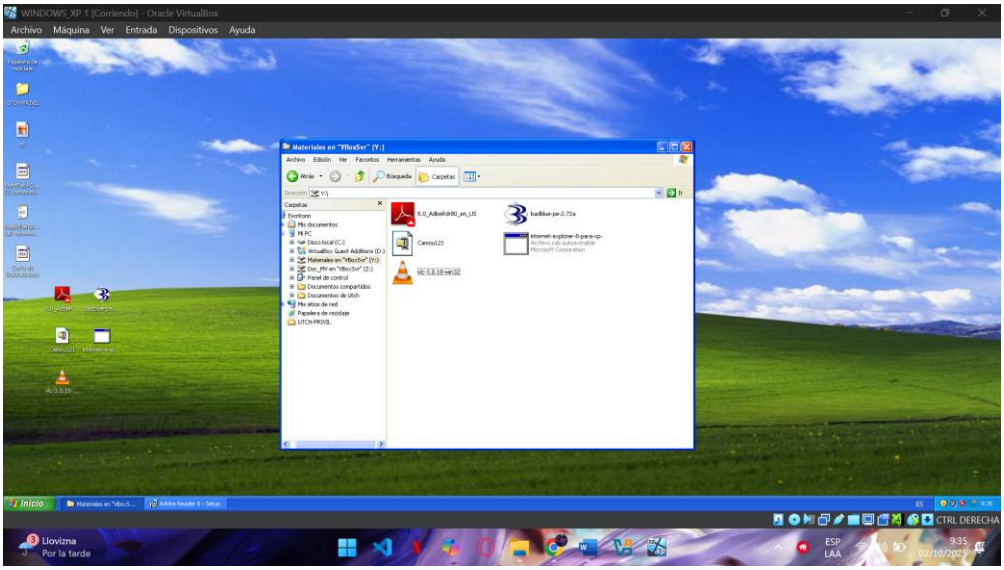
5. Selección de la carpeta compartida desde el sistema anfitrión

Aquí se configura la ruta de la carpeta compartida, seleccionando **Doc_MV** desde la ruta local **C:\Users\Edward Camilo\Downloads**. Este paso vincula la carpeta del sistema anfitrión con la máquina virtual, habilitando la comunicación de archivos de manera directa. se activa el modo **Automontar** y se marca la opción **Hacer permanente**, garantizando que la carpeta esté disponible cada vez que se inicie la máquina virtual.



6. Configuración de los parámetros de la carpeta compartida

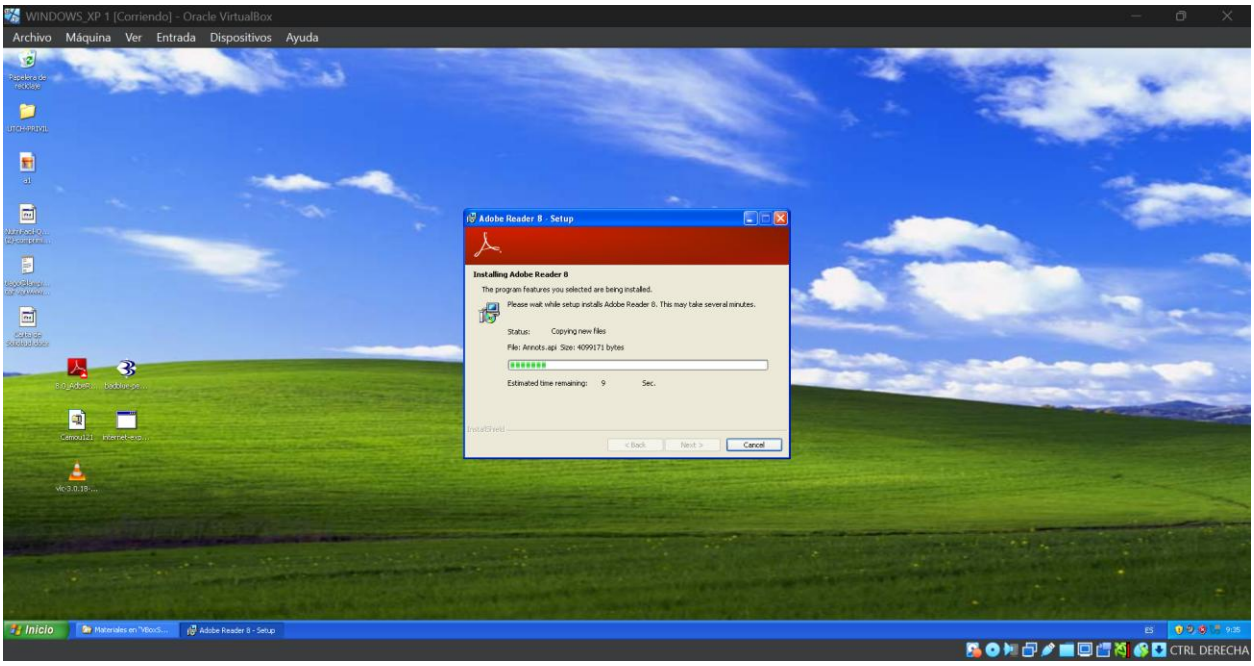
Finalmente, se muestra que la carpeta **Doc_MV** ha sido montada exitosamente dentro del sistema operativo **Windows XP**, visible como una unidad de red con el identificador **Z:** bajo el nombre *VBoxSvr*. Esto confirma la correcta comunicación entre el sistema anfitrión y la máquina virtual.



7. Configuración de los parámetros de la carpeta compartida.

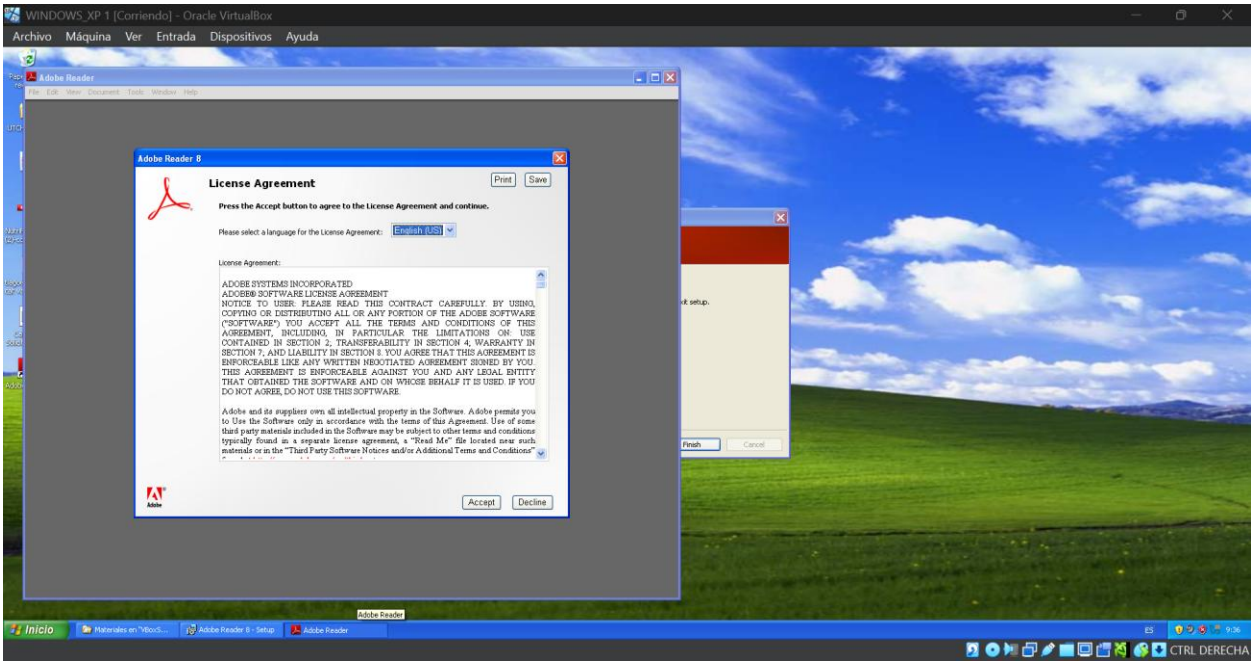
Paso 3: Instalación de los programas pasados a Windows xp

Se muestra el proceso de instalación del programa **Adobe Reader 8** en el sistema operativo **Windows XP** mediante la máquina virtual Oracle VirtualBox



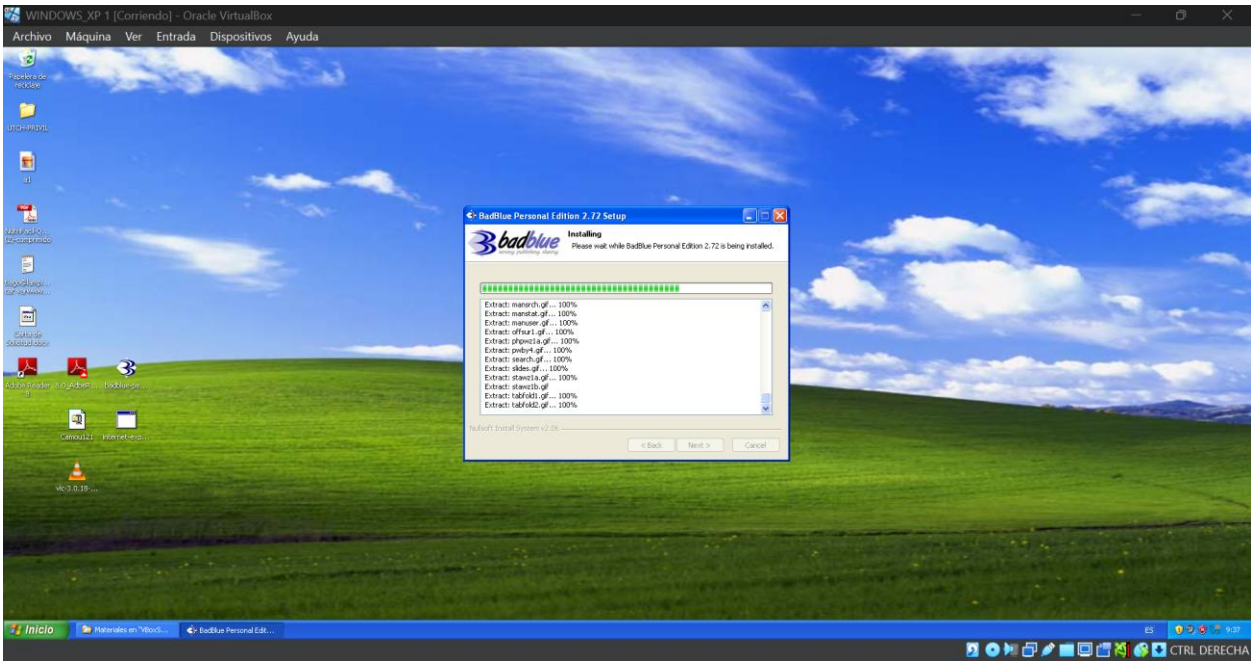
8. Instalación de Adobe Reader 8

Ventana correspondiente al **acuerdo de licencia** del programa **Adobe Reader 8**. El usuario debe aceptar los términos y condiciones establecidos por Adobe Systems para continuar con la instalación del software.



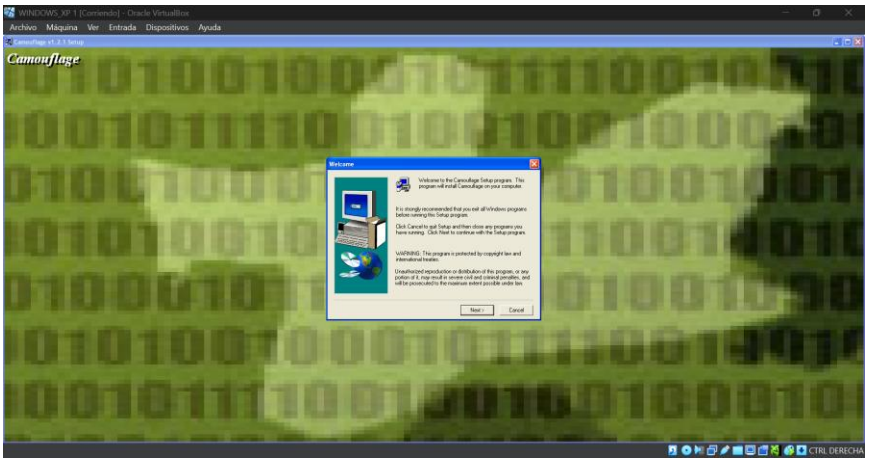
9. Aceptación del acuerdo de licencia de Adobe Reader 8

Captura del proceso de instalación del software **BadBlue Personal Edition 2.72**, herramienta utilizada para compartir archivos y servir contenido web en redes locales. Se observa el avance de la extracción e instalación de archivos en el entorno Windows XP.



10. Instalación de BadBlue Personal Edition 2.72

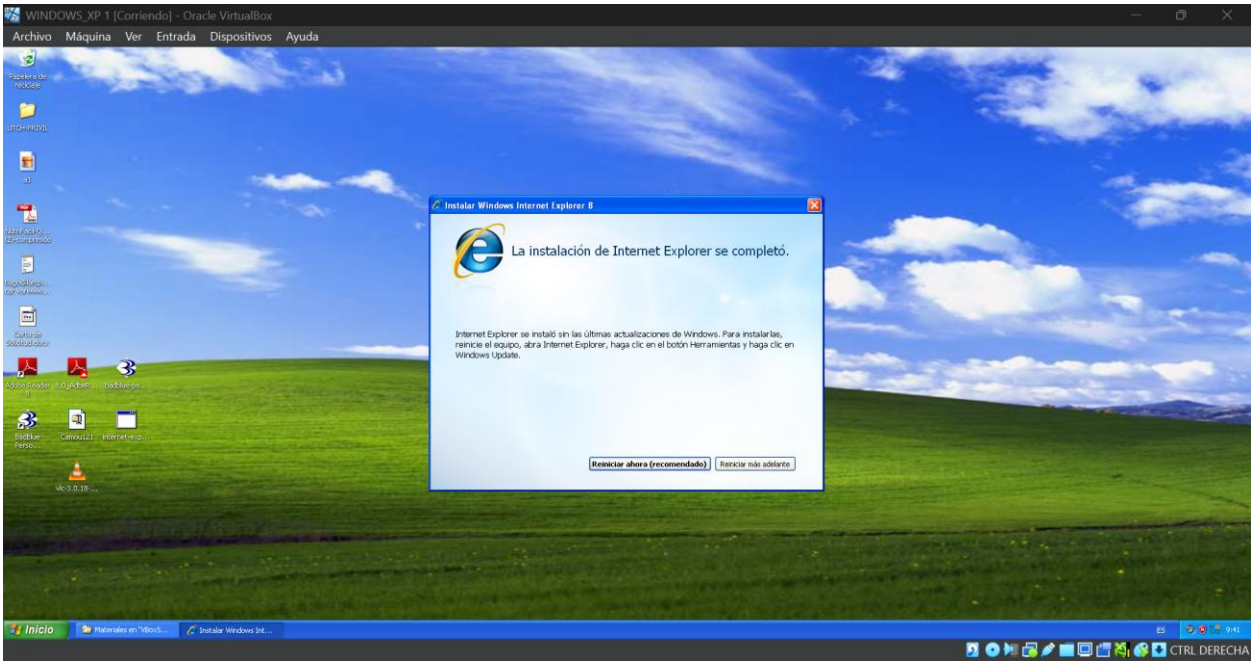
Inicio del asistente de instalación del programa **Camouflage 1.2.1**, una aplicación empleada para ocultar archivos dentro de otros, brindando una capa adicional de seguridad mediante esteganografía. Se muestra la pantalla de bienvenida del instalador.



11. Instalación del programa Camouflage 1.2.1

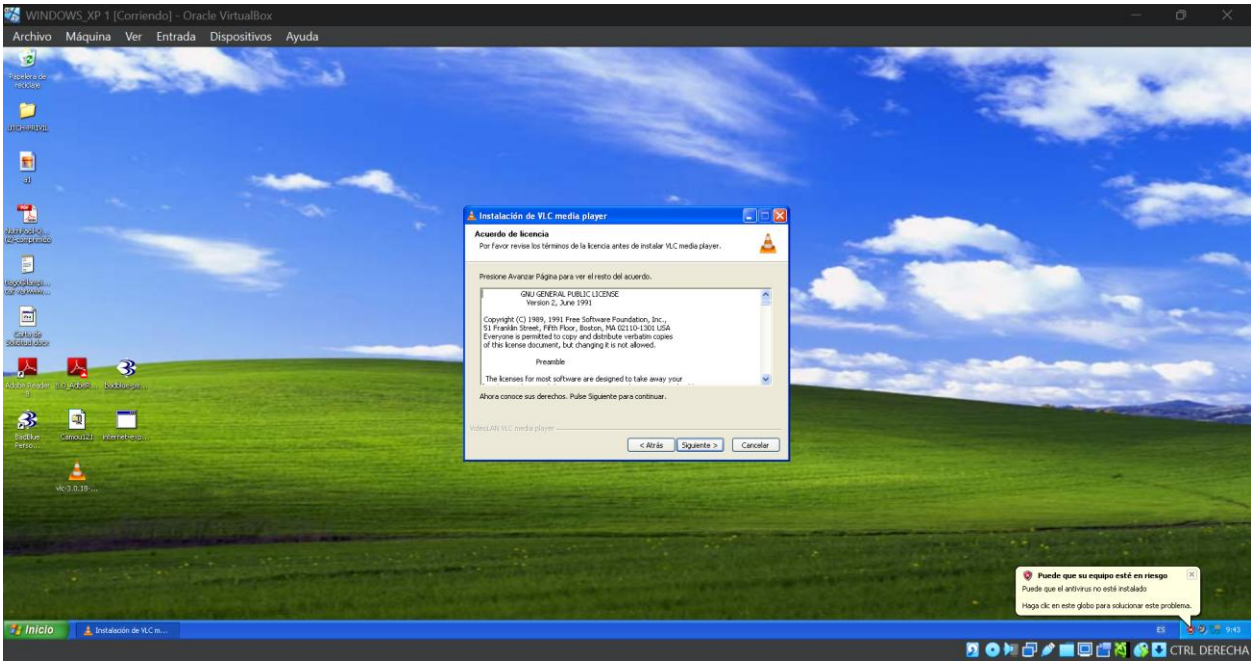
Proceso de instalación del navegador **Internet Explorer 8** en Windows XP. En esta fase, el sistema descarga actualizaciones y archivos necesarios para completar la instalación del explorador de Microsoft.

12. Instalación de Windows Internet Explorer 8



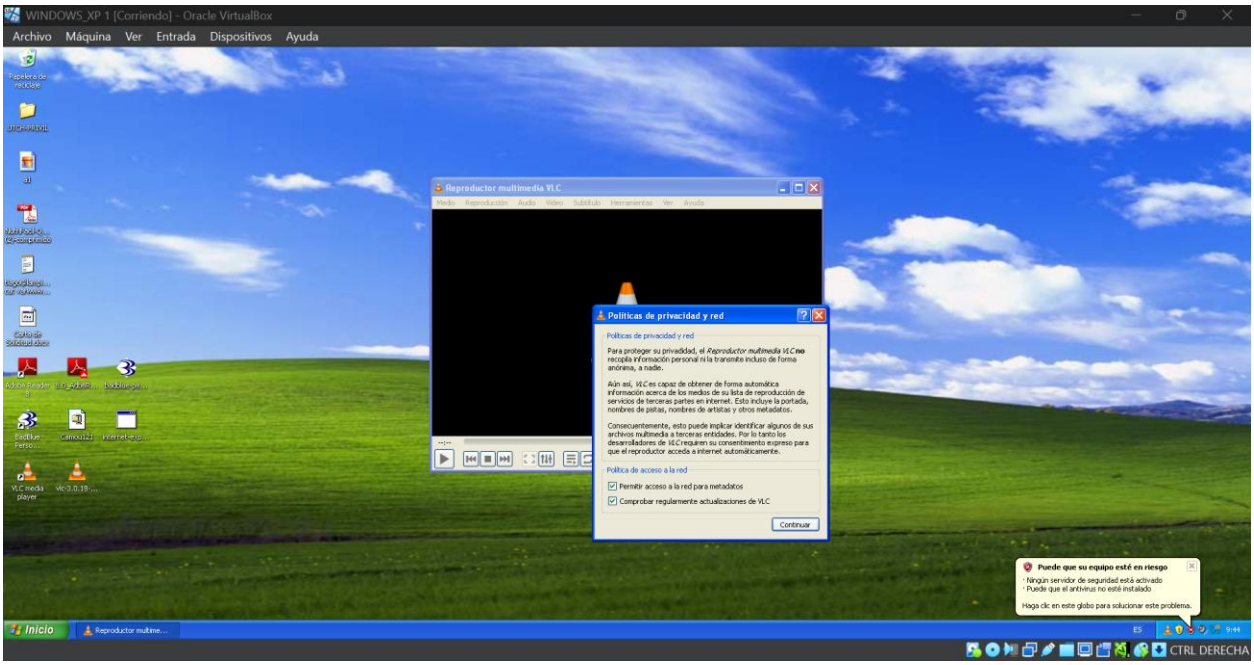
13. Instalación Finalizada

Primera ejecución del programa **VLC Media Player** tras su instalación. Se visualiza la ventana de configuración de las **políticas de privacidad y red**, donde el usuario puede habilitar el acceso a metadatos y actualizaciones automáticas.



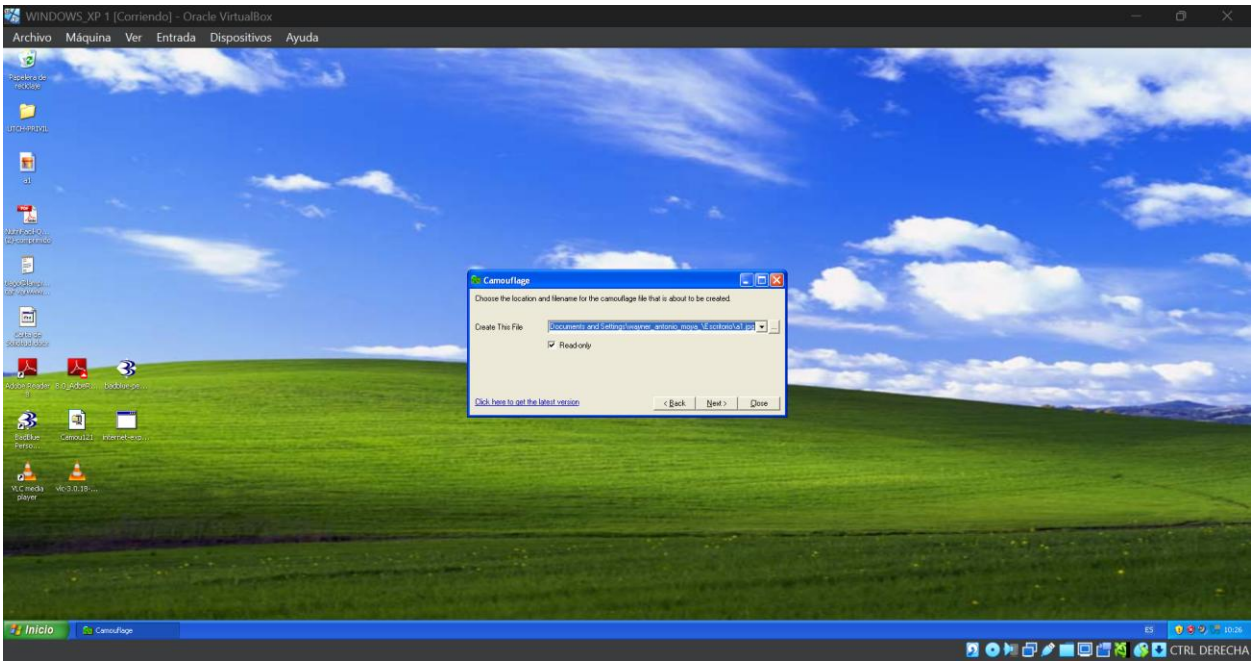
14. Configuración inicial del reproductor multimedia VLC

Primera ejecución del programa **VLC Media Player** tras su instalación. Se visualiza la ventana de configuración de las **políticas de privacidad y red**, donde el usuario puede habilitar el acceso a metadatos y actualizaciones automáticas.



15. Configuración inicial del reproductor multimedia VLC

Paso 4 Se visualiza la interfaz del programa **Camouflage** durante el proceso de creación de un archivo camuflado. En esta etapa, el usuario define la ubicación y el nombre del archivo resultante que contendrá los datos ocultos.



16. Creación del archivo camuflado con Camouflage

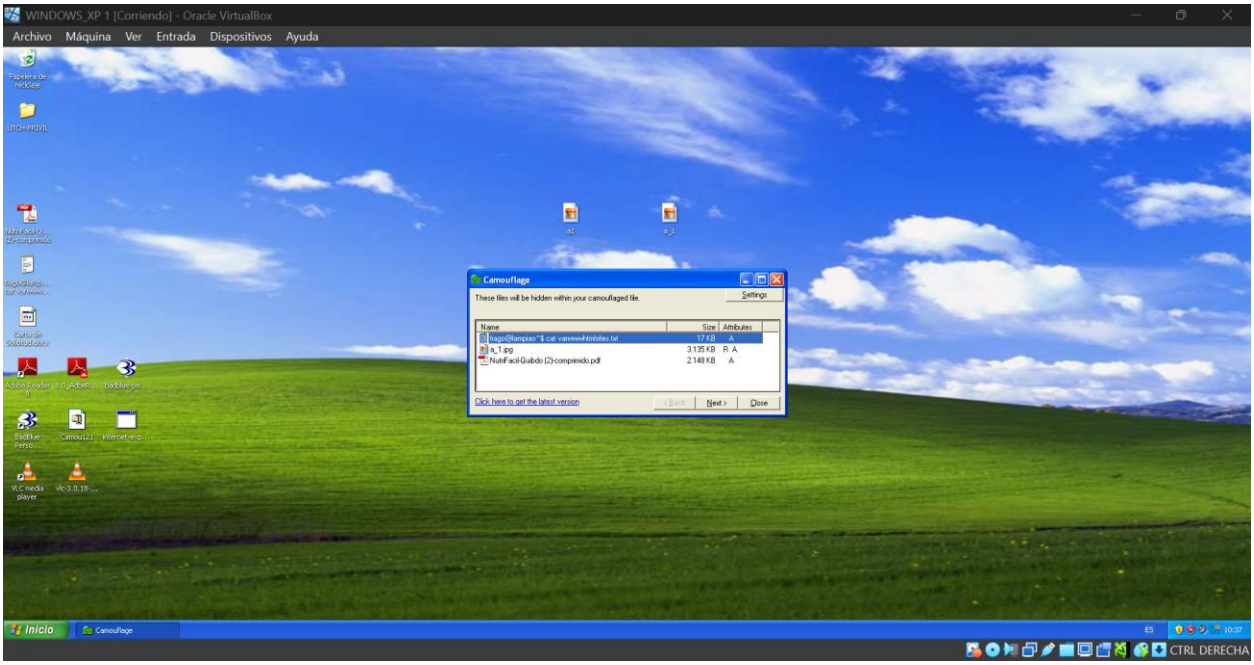
Se muestran en el escritorio los archivos originales antes del proceso de camuflaje. Estos archivos servirán como base para la ocultación de información mediante la herramienta Camouflage.

17. Archivos visibles en el escritorio de Windows XP

El usuario realiza un clic derecho sobre un archivo con el fin de abrir el menú contextual y seleccionar la opción de Camouflage, dando inicio al proceso de ocultamiento de archivos dentro de otro.

18. Selección del archivo portador para el camuflaje

La interfaz de Camouflage muestra los archivos que serán ocultos dentro del archivo principal. En este caso, se observan varios documentos listos para ser incorporados al archivo camuflado.

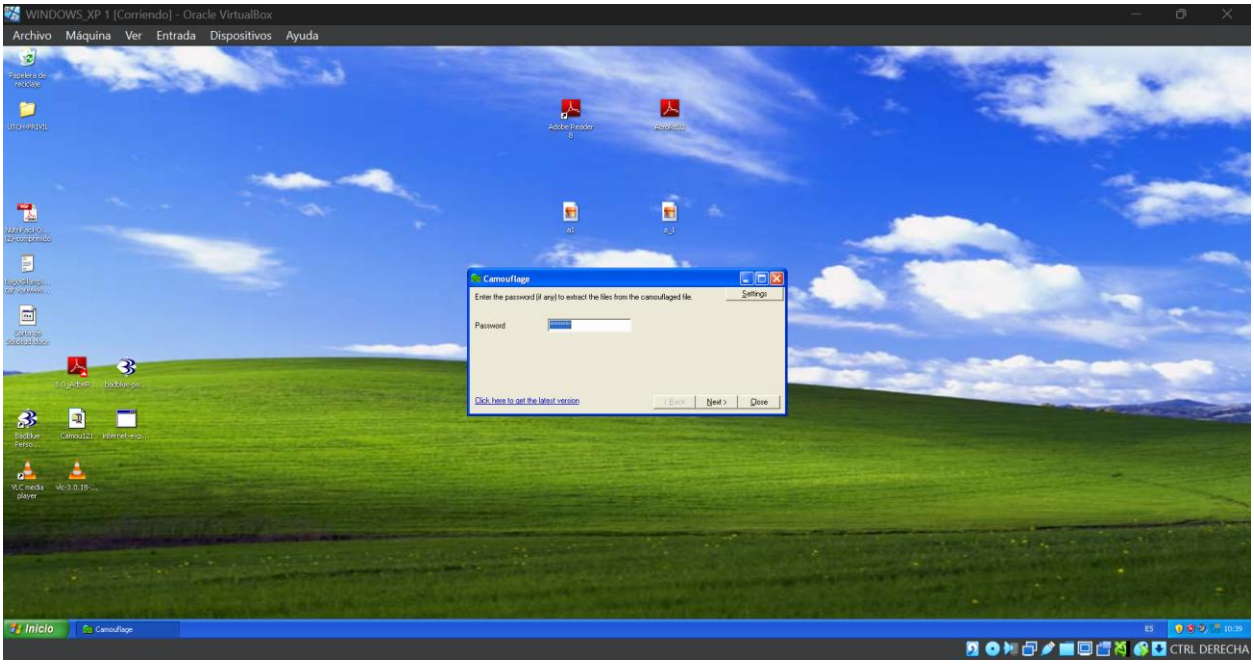


19. Ventana de selección de archivos para ocultar

Se aprecia el escritorio de Windows XP tras finalizar el proceso de camuflaje, donde los archivos ocultos se encuentran integrados dentro de un archivo portador que mantiene su apariencia original.

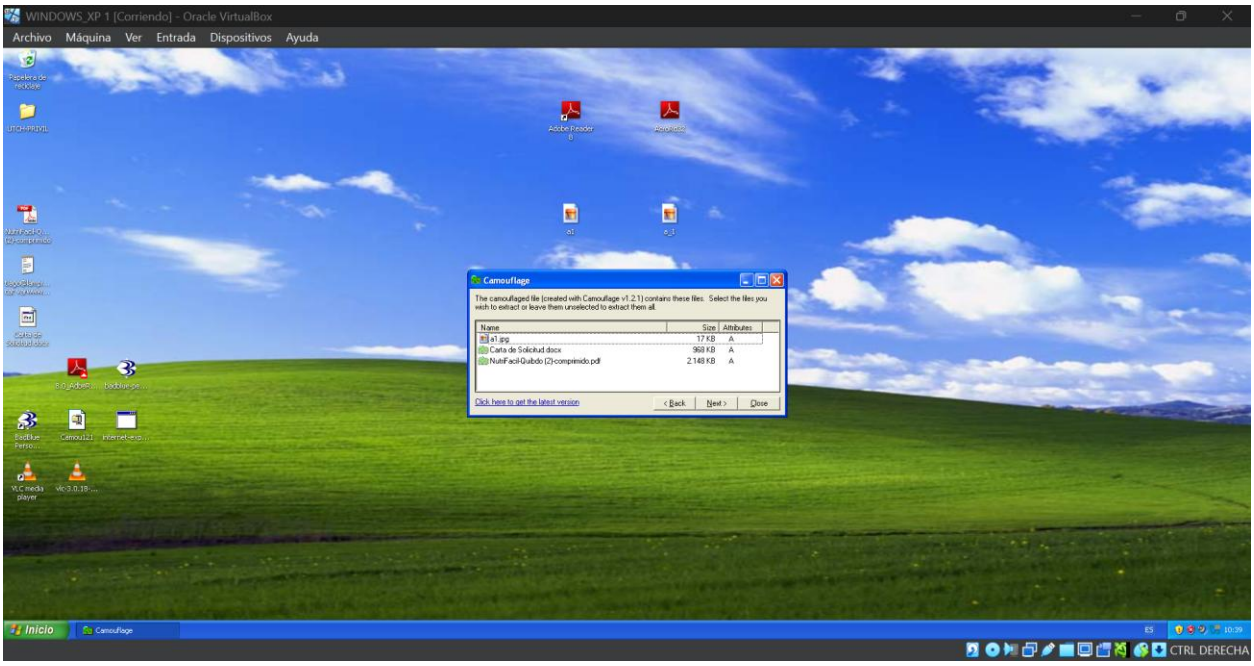
20. Archivos camuflados en el escritorio

Camouflage solicita al usuario la **contraseña de seguridad** necesaria para acceder al contenido oculto dentro del archivo camuflado, asegurando así la confidencialidad de la información.



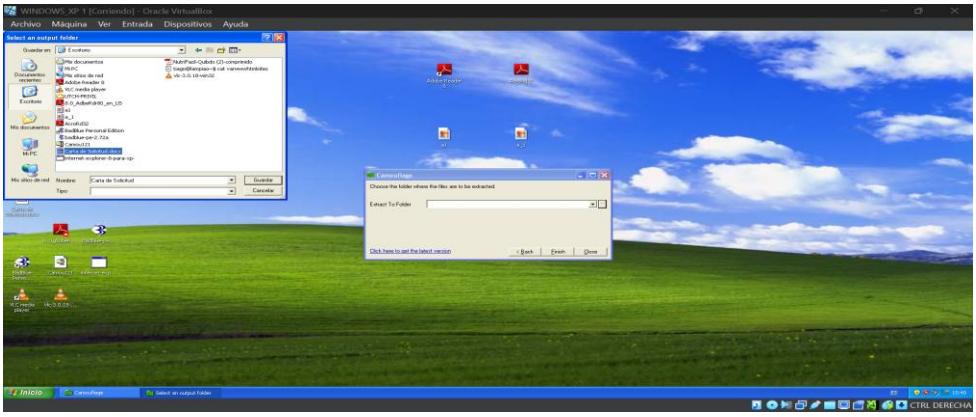
21. Ingreso de contraseña para extraer archivos

Ventana final del programa **Camouflage** mostrando los archivos extraídos con éxito desde el archivo camuflado. Este proceso demuestra la recuperación de información protegida mediante esteganografía.



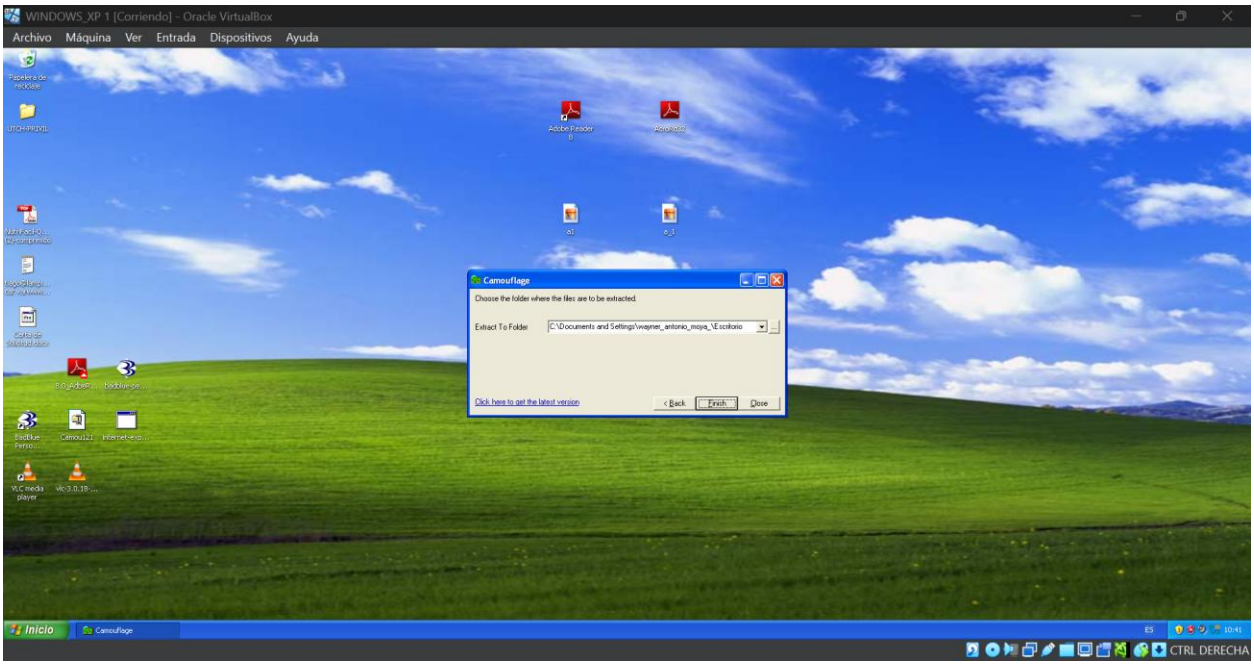
22. Extracción de archivos desde el archivo camuflado

El programa **Camouflage** solicita al usuario seleccionar la ubicación donde se guardarán los archivos extraídos del archivo camuflado. En esta ventana se puede definir una carpeta específica dentro del sistema operativo Windows XP.



23. Selección de carpeta de destino para la extracción

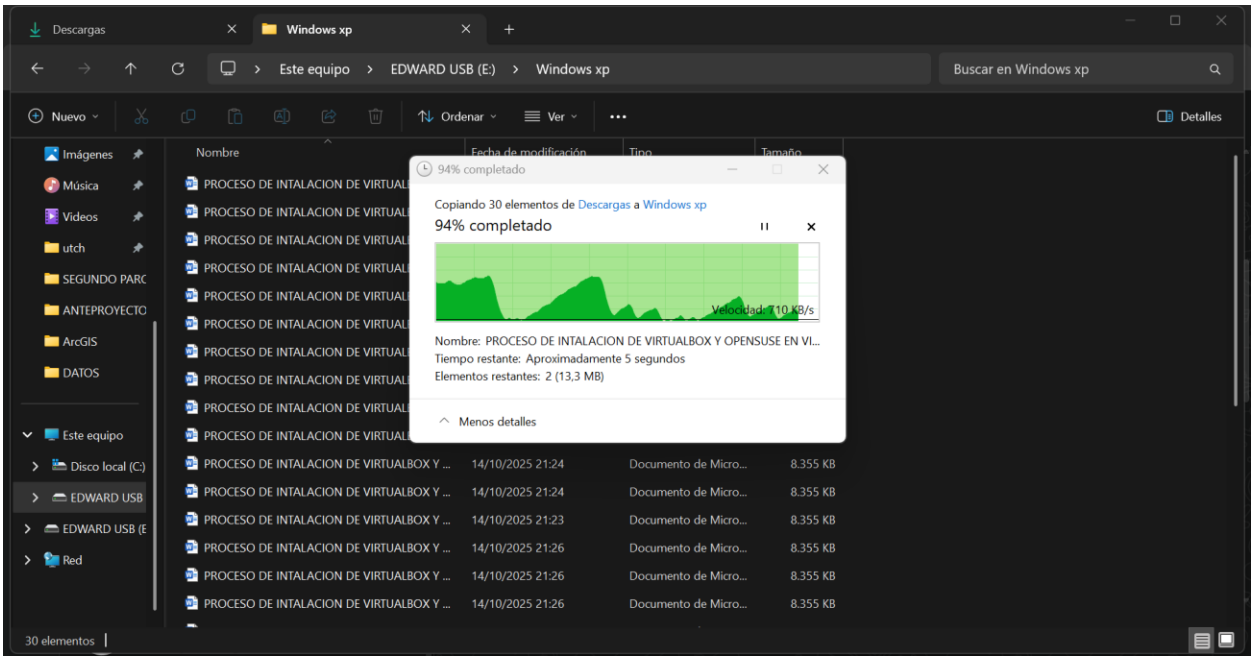
Se muestra la ventana de confirmación de la ruta seleccionada para extraer los archivos ocultos mediante **Camouflage**. Al presionar el botón “Finish”, el programa procede a recuperar los datos en la ubicación indicada.



24. Confirmación de la carpeta de extracción

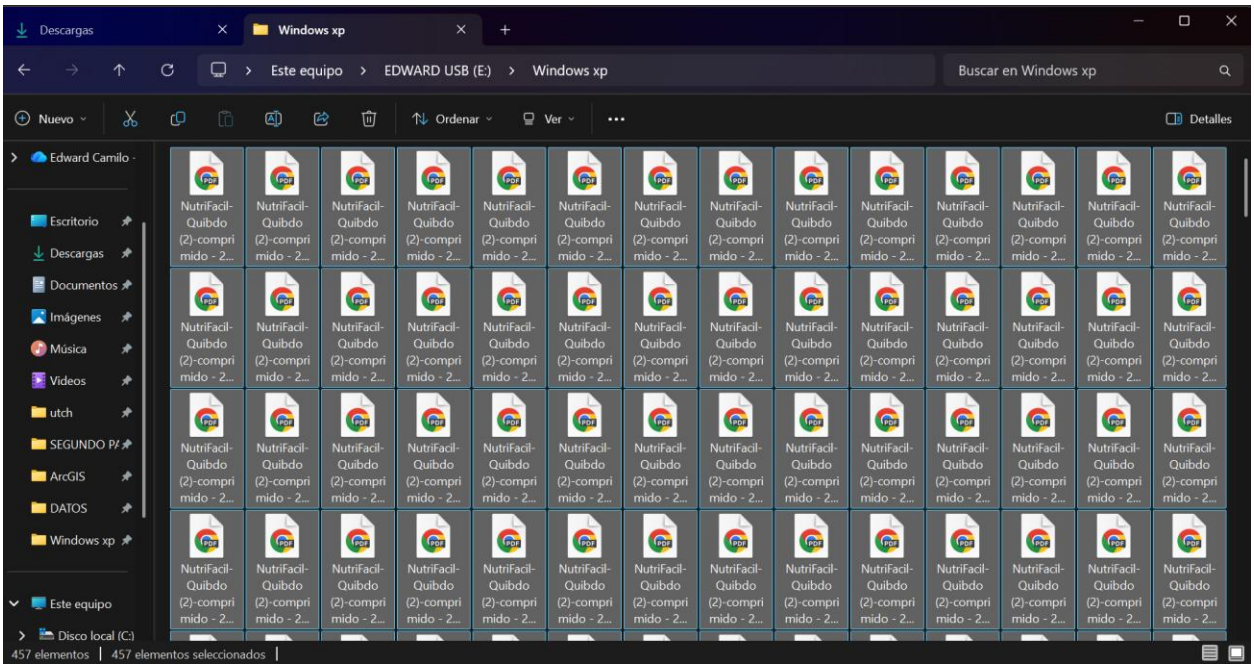
CAPITULO 1 LIMITE DE CAMUFLAGE DE ARCHIVOS

Se muestra la copia de documentos relacionados con el proceso de instalación de VirtualBox y OpenSUSE hacia la carpeta “Windows XP”, preparando los archivos necesarios para el laboratorio de camuflaje.



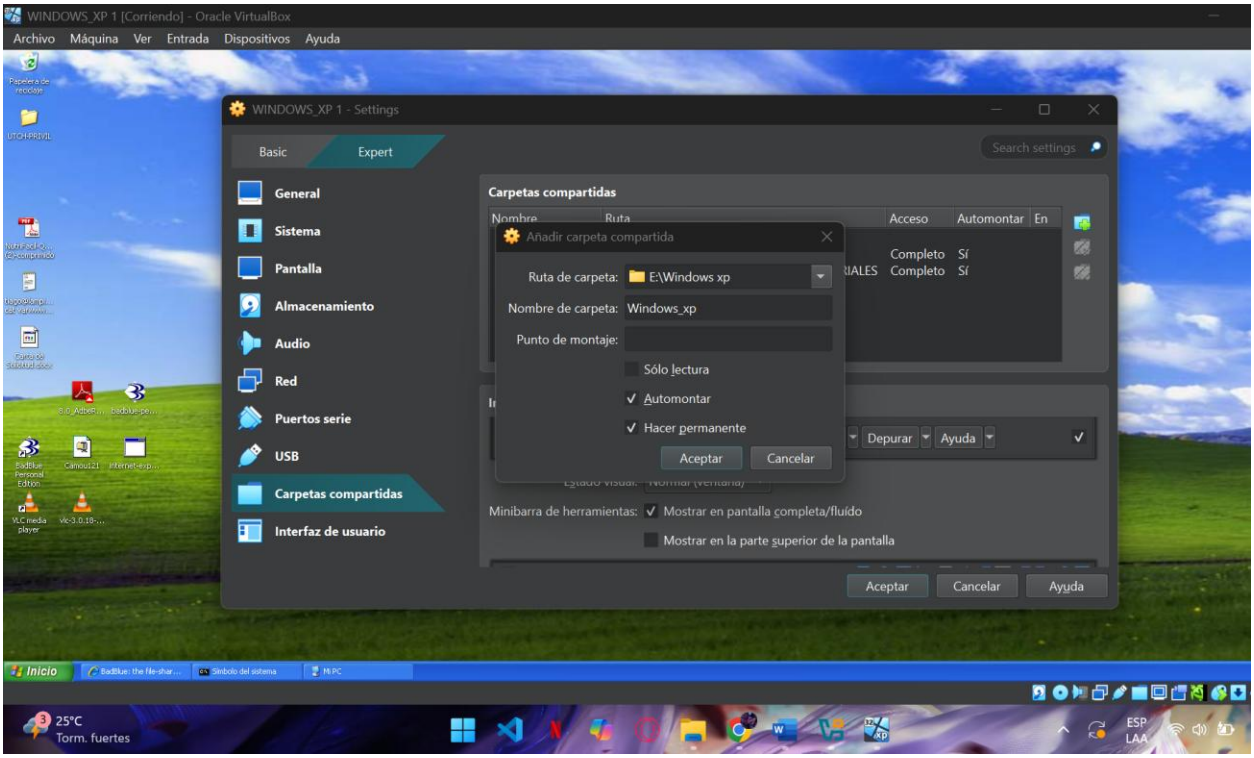
25Transferencia de archivos para el entorno virtual

Carpeta “Windows XP” con múltiples archivos copiados exitosamente, los cuales se utilizarán para las pruebas de camuflaje en el entorno de Windows XP virtualizado.



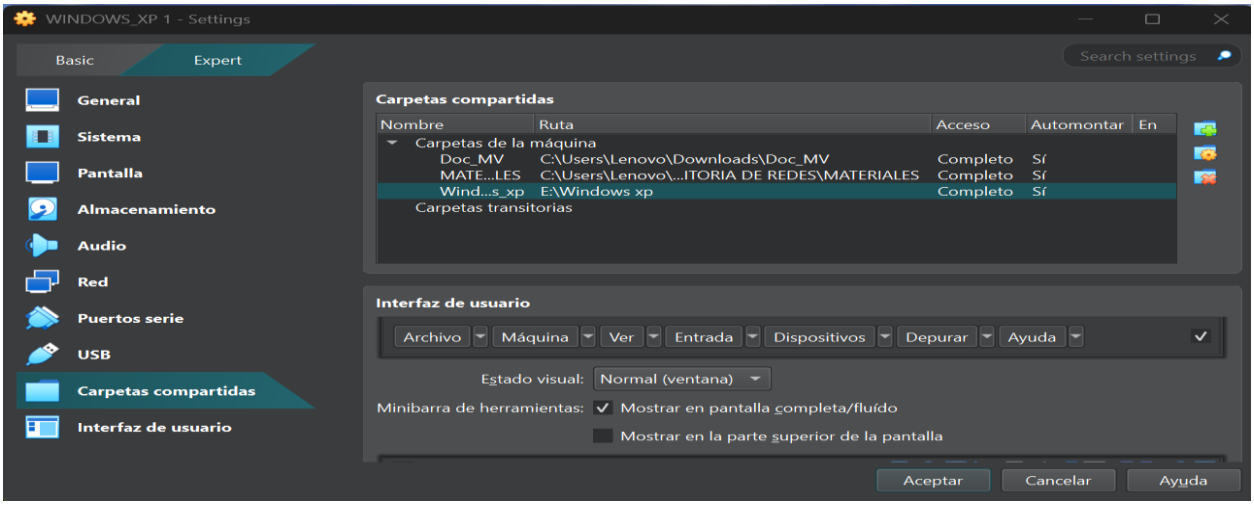
26. Verificación de archivos copiados

Ajuste de la carpeta compartida “Windows xp” en VirtualBox para permitir la conexión entre el sistema anfitrión y la máquina virtual, facilitando el intercambio de archivos.



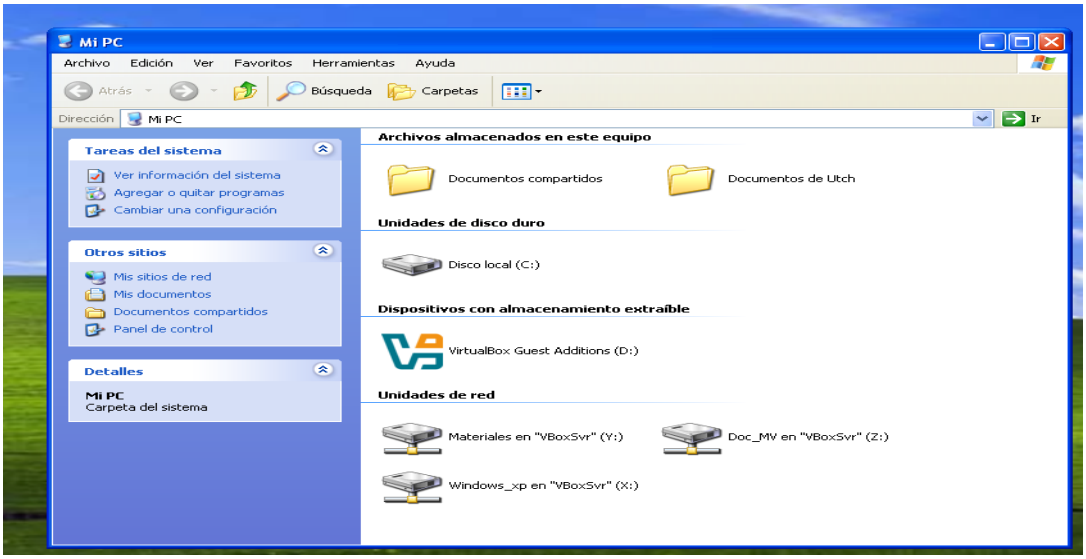
27. Configuración de carpeta compartida en VirtualBox

Se observa en la configuración avanzada de VirtualBox la carpeta “Windows xp” agregada con acceso completo y auto montaje activado, confirmando la correcta conexión entre sistemas.



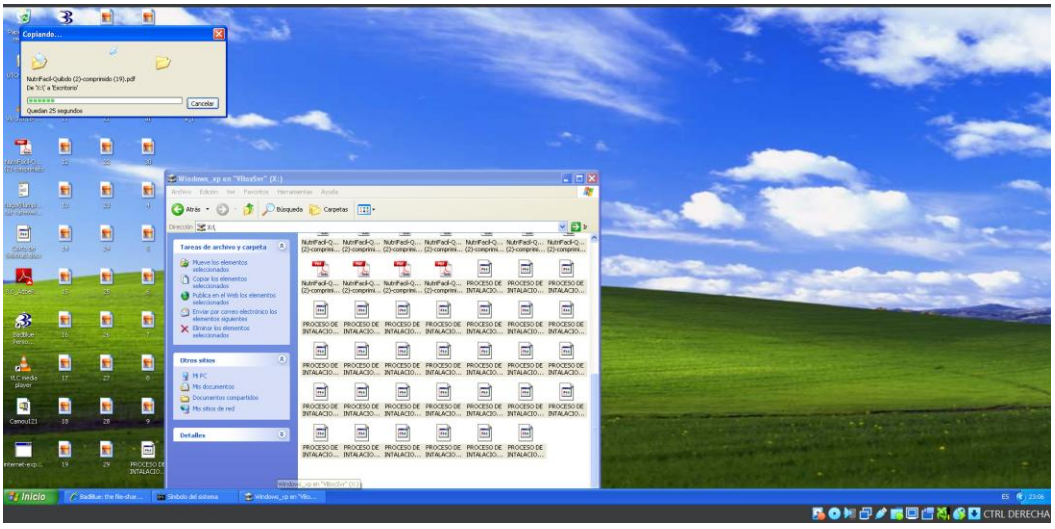
28. Carpeta compartida configurada correctamente

Dentro de la máquina virtual, Windows XP detecta correctamente las unidades compartidas (X:, Y:, Z:), confirmando la comunicación con el equipo anfitrión.



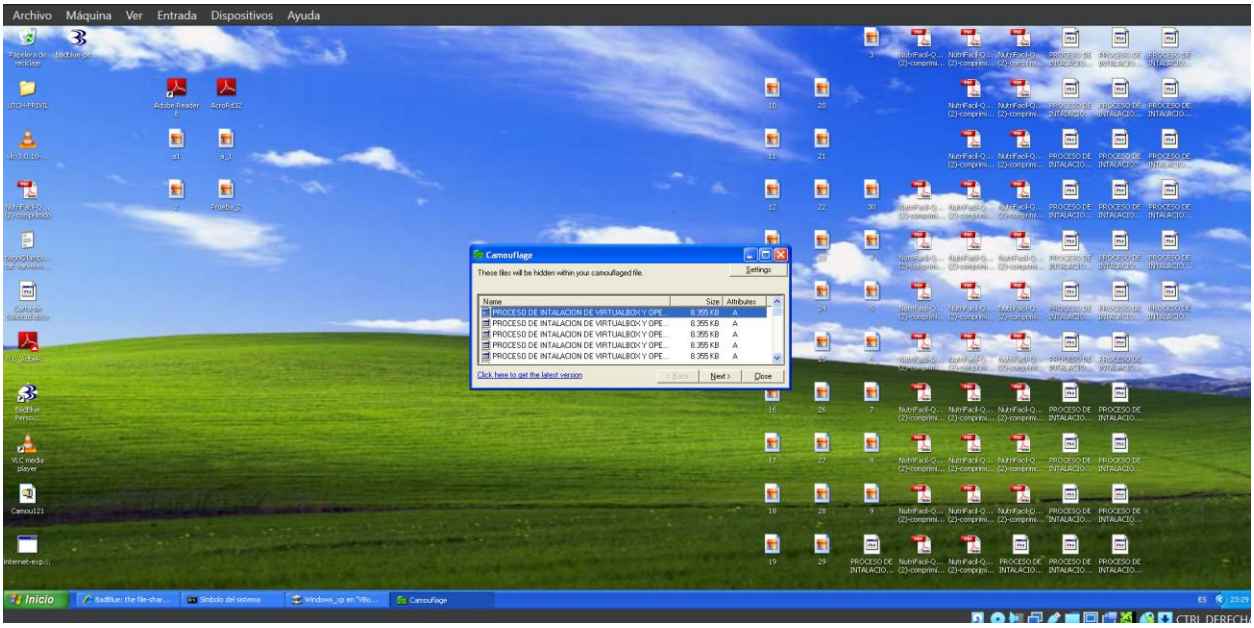
29. Acceso a carpetas compartidas desde Windows XP

Transferencia de los documentos desde la carpeta compartida hacia el escritorio de Windows XP, asegurando la disponibilidad de los archivos dentro del entorno virtualizado.



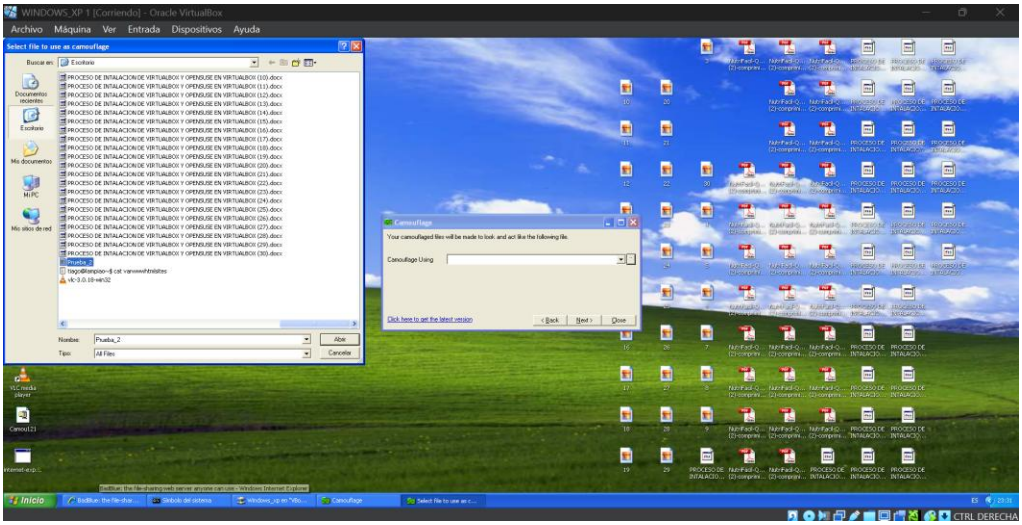
30. Copia de archivos al entorno virtual

Vista general del escritorio de Windows XP mostrando los archivos de prueba y documentos PDF que serán utilizados en el proceso de camuflaje con la herramienta Camouflage.



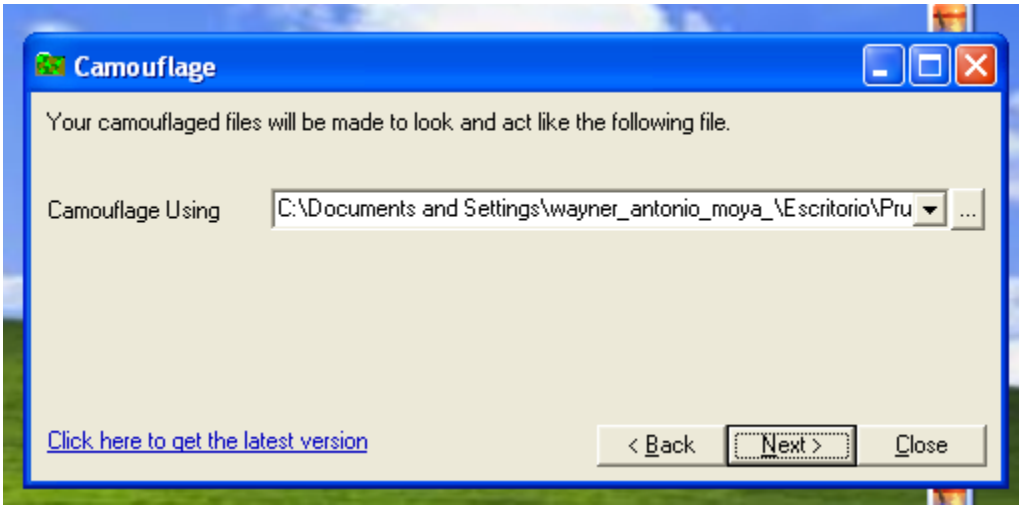
31. Archivos listos para camuflaje

La interfaz de Camouflage permite elegir el archivo que actuará como contenedor, dentro del cual se ocultarán los demás archivos seleccionados.



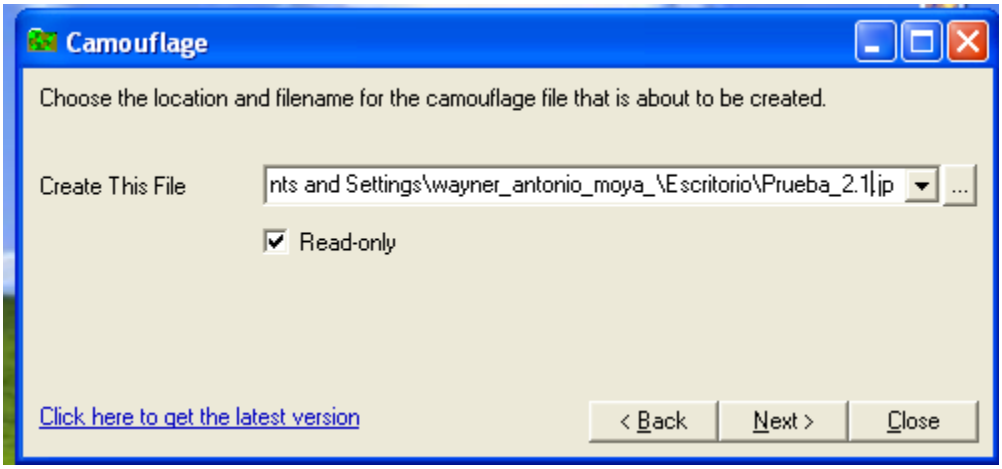
32. Configuración del archivo contenedor

Se observa la ruta del archivo contenedor configurado en el programa Camouflage, que servirá como camuflaje para los archivos seleccionados.



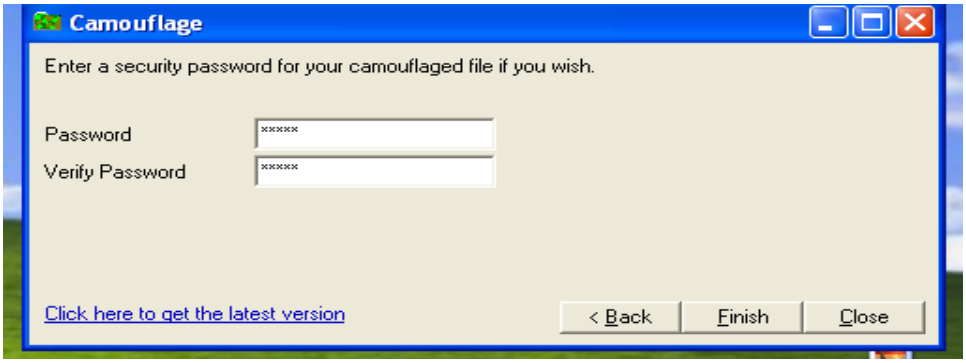
33. Archivo contenedor definido en Camouflage

En esta ventana del programa *Camouflage*, se selecciona la ubicación y el nombre del archivo que será creado con la información oculta. Se puede observar que se activa la opción "Solo lectura" antes de continuar con el proceso.



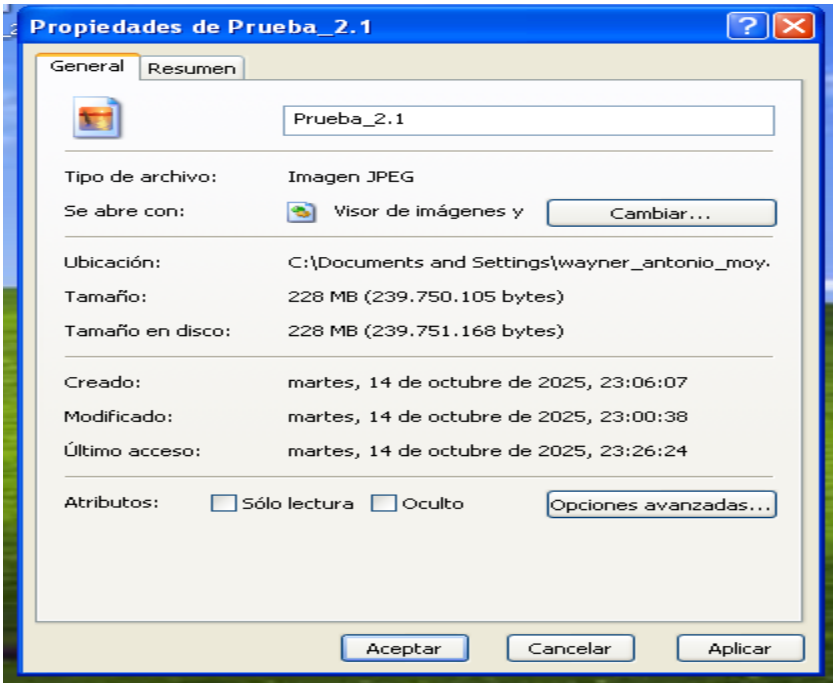
34. Creación del archivo camuflado

El programa solicita establecer una contraseña de seguridad para proteger el archivo camuflado. En este caso, se utilizó la contraseña **54321** para continuar con la encriptación del contenido.



35. Configuración de contraseña

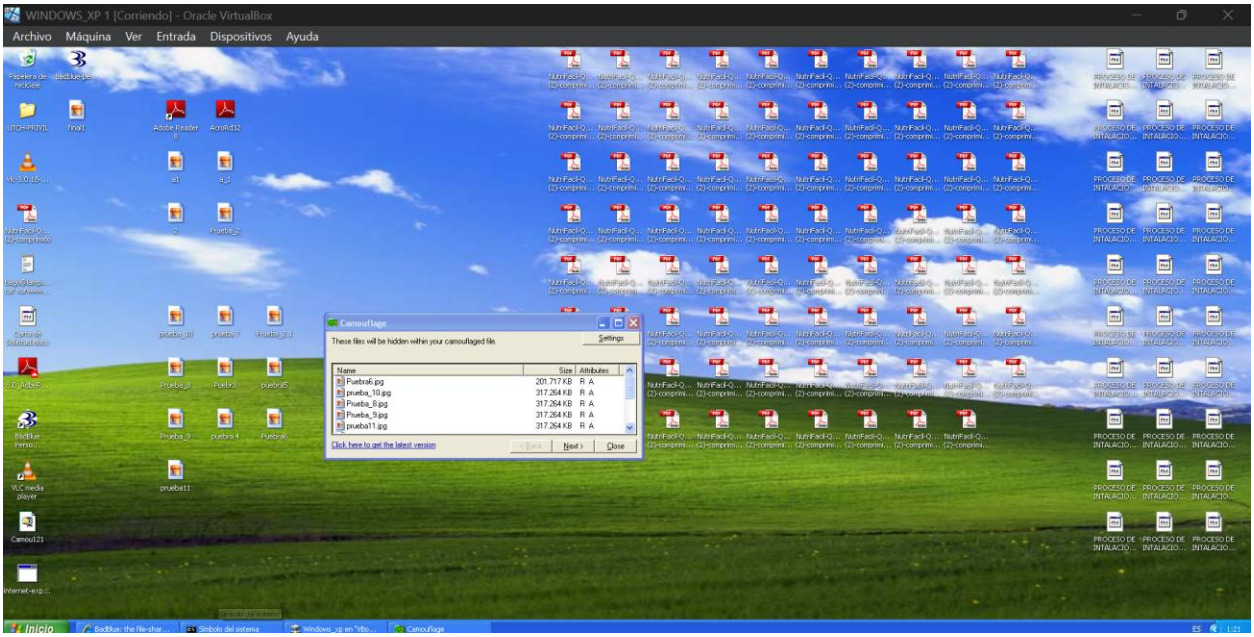
Aquí se muestran las propiedades del archivo generado llamado **Prueba_2.1**, identificado como una imagen JPEG con un tamaño de **228 MB**. Esto indica que los datos se ocultaron correctamente dentro del archivo de imagen.



36. Propiedades del archivo resultante

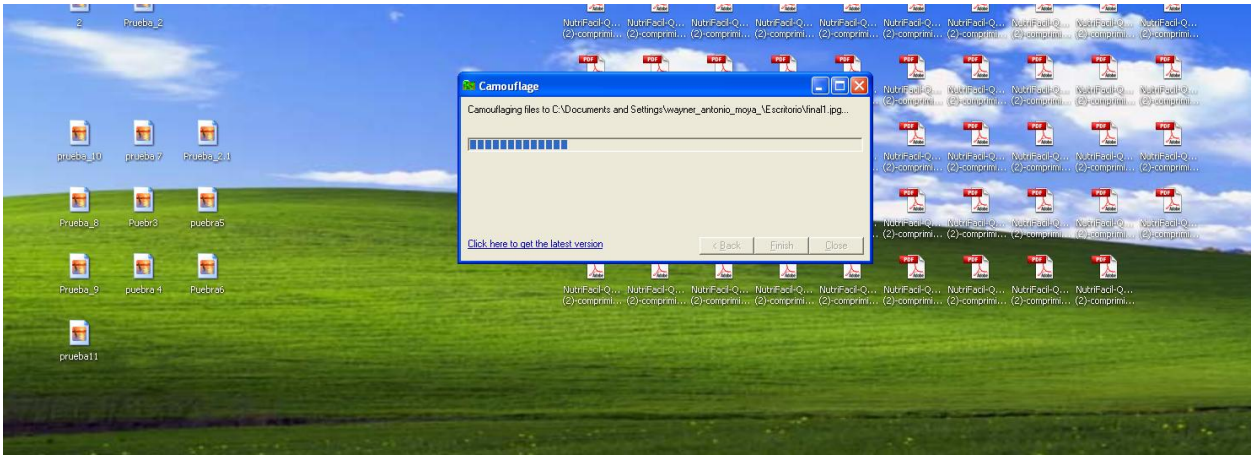
En esta captura se observa el escritorio del sistema operativo Windows XP ejecutándose en *VirtualBox*. Se puede ver que el sistema comienza a mostrar señales de lentitud mientras se procesan varios archivos con Camouflage.

Desde aquí muestra sinos de lentitud



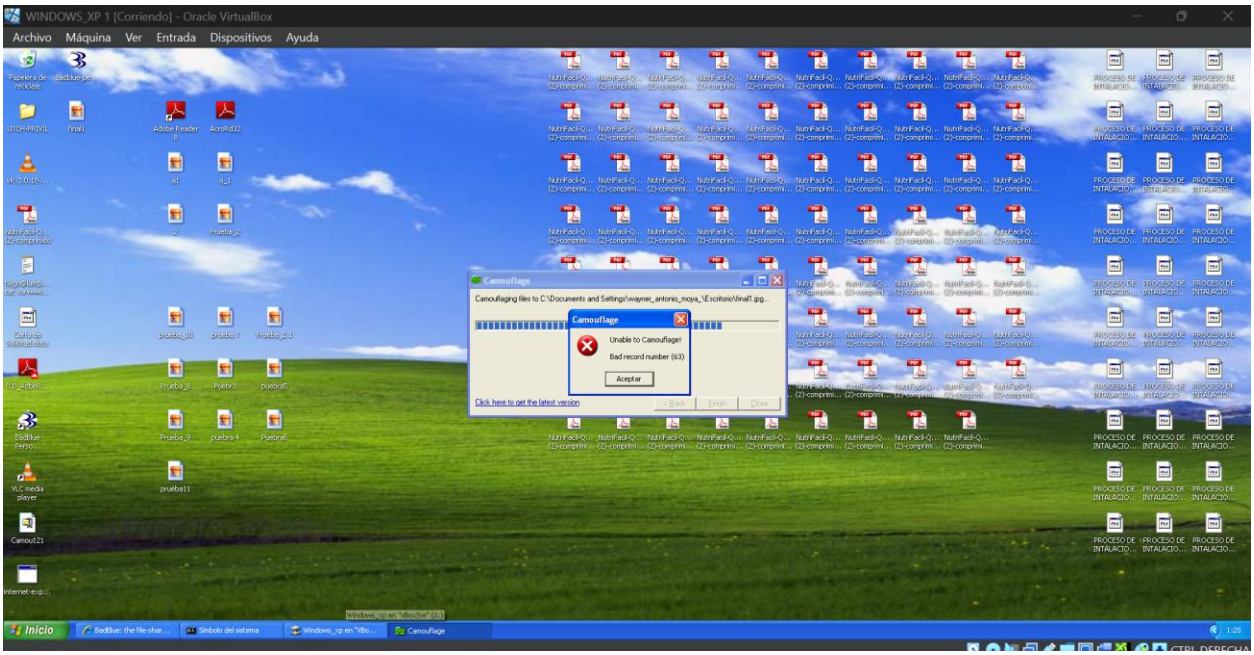
37. Ejecución del programa Camouflage

El programa *Camouflage* está realizando el proceso de ocultar información dentro del archivo especificado. La barra de progreso muestra el avance de la operación mientras se crea el archivo camuflado.



38. Proceso de camuflaje en ejecución

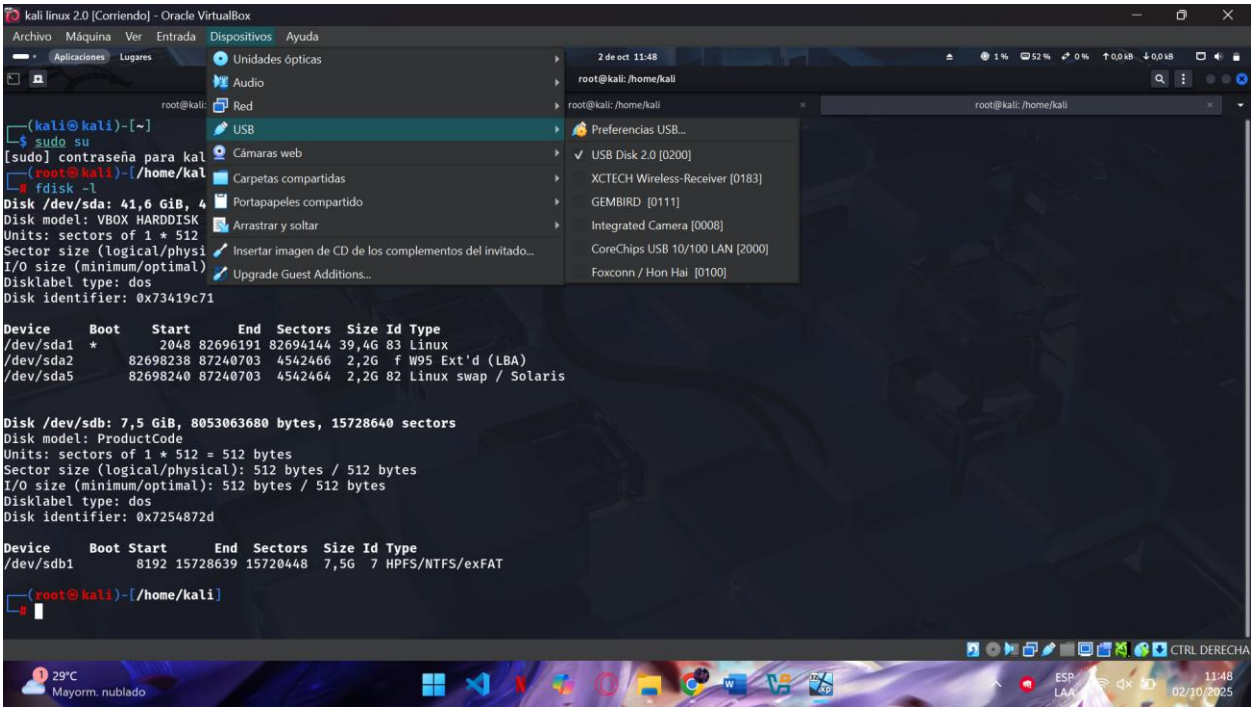
Durante la creación del archivo final, el programa muestra un error con el mensaje *"Bad record number (63)"*. Esto indica que el proceso no se completó correctamente, probablemente debido al tamaño o tipo del archivo utilizado.



39. Error durante el proceso de camuflaje

CAPITULO 2: HASH

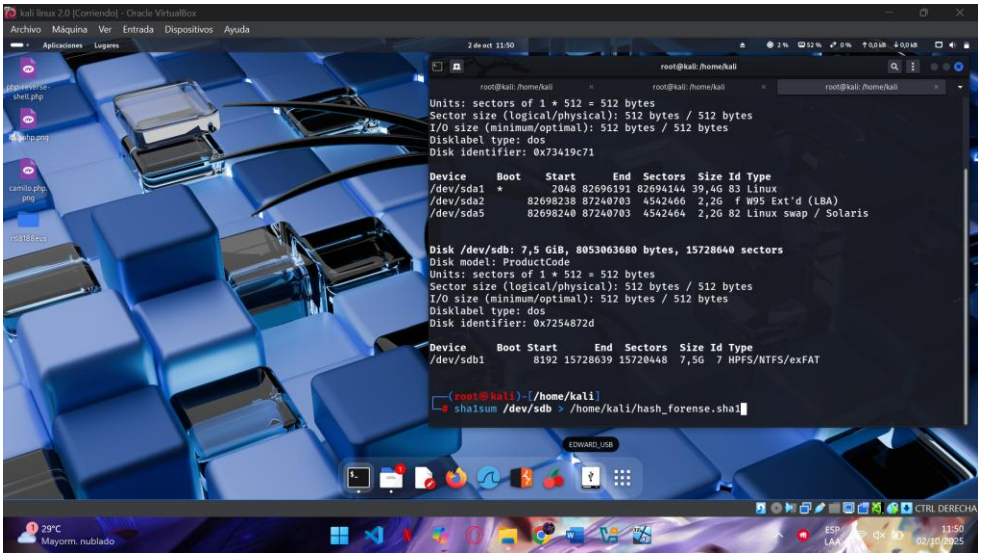
Se muestra el sistema operativo *Kali Linux 2.0* corriendo en *VirtualBox*. En la parte superior se selecciona el dispositivo USB desde el menú para conectarlo a la máquina virtual. En la terminal se ejecuta el comando fdisk -l para listar los discos conectados y verificar la detección del USB.



40. Conexión del dispositivo USB en Kali Linux

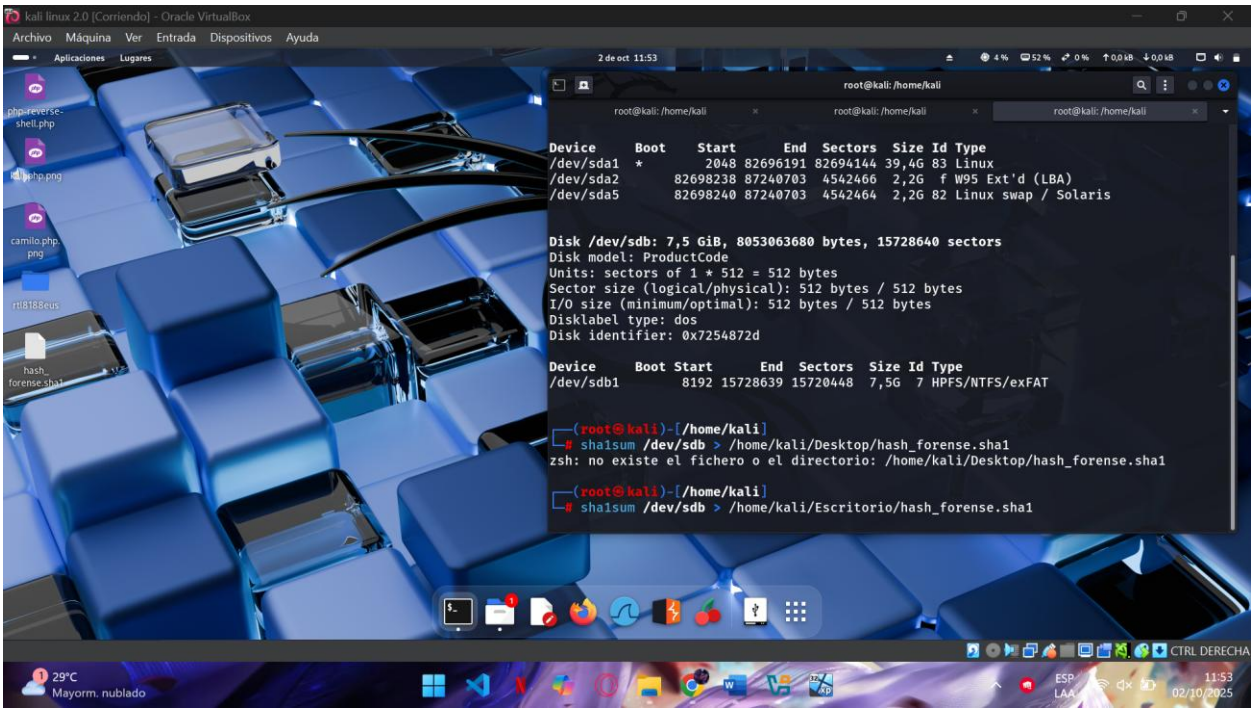
En esta imagen se utiliza el comando sha1sum para generar el hash del dispositivo /dev/sdb. El resultado se guarda en un archivo llamado **hash_forense.sha1** ubicado en la carpeta **/home/kali**.

Este hash sirve para comprobar la integridad de los datos del dispositivo USB.



41. Creación del archivo hash forense

Después de un intento fallido de guardar el archivo hash en una carpeta inexistente, se corrige la ruta y se almacena el archivo **hash_forense.sha1** en el **Escritorio**. Esto permite un acceso más rápido y una mejor organización de la evidencia digital generada.



42. Guardado correcto del hash en el escritorio

CAPITULO 3: BADBLUE

Salida de nmap -sV 10.0.2.7 que muestra puerto 80 abierto y servicio **BadBlue httpd 2.7**, junto con otros puertos de Windows. Esto confirma la presencia del servidor vulnerable y su versión.

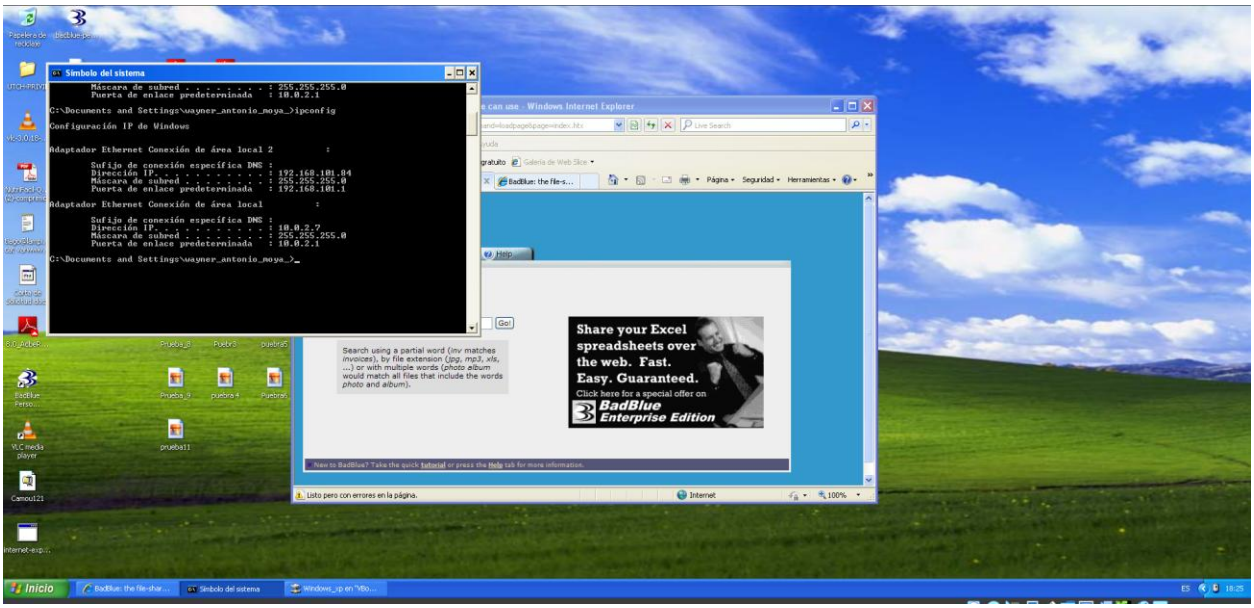
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 18:17 -05
Nmap scan report for 10.0.2.7
Host is up (0.0028s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
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 NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.81 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

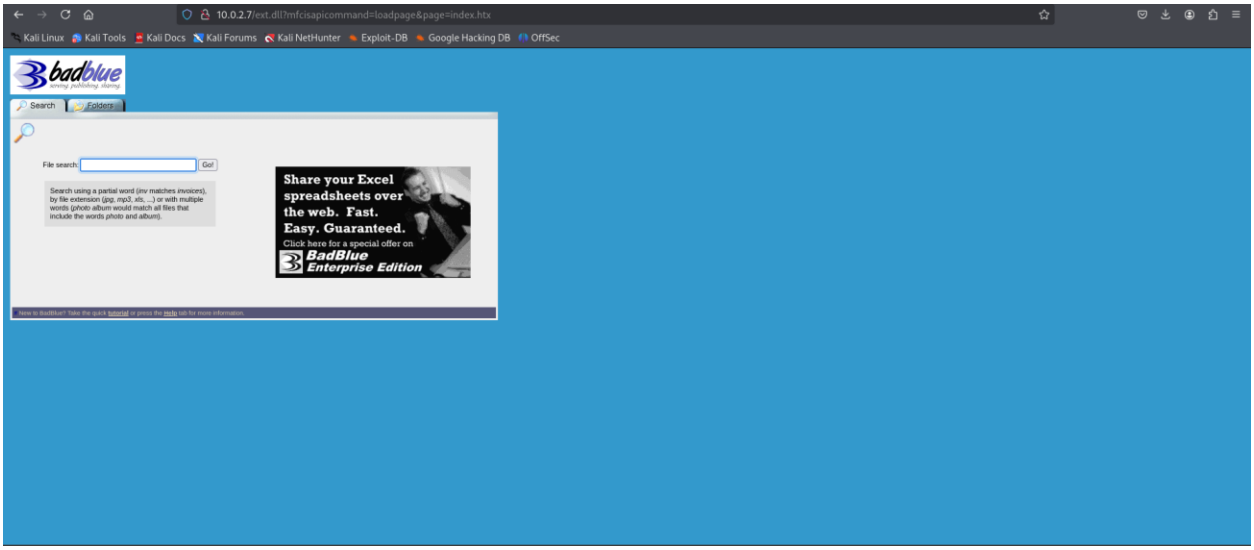
43. Detección del servicio con Nmap

Captura del escritorio Windows XP donde se observa una ventana de símbolo del sistema (ipconfig) y el navegador apuntando a la interfaz de BadBlue. Muestra que el host objetivo responde en la red y la página web del servicio es accesible desde la máquina de pruebas.



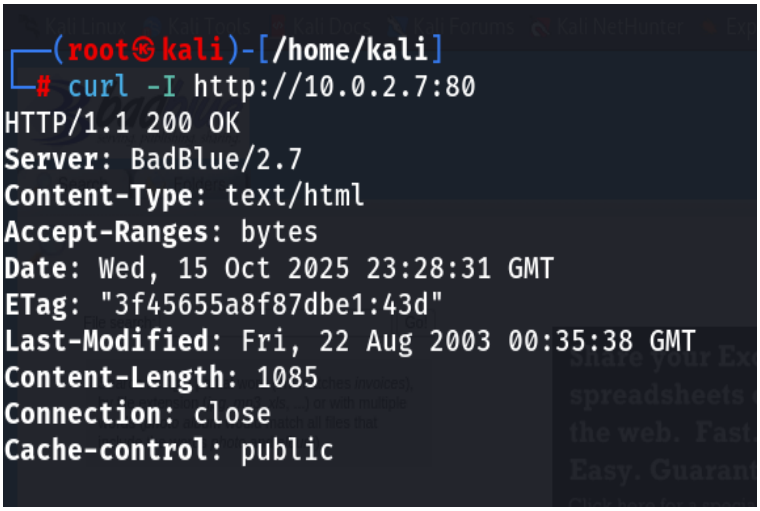
44,Acceso al equipo objetivo (escritorio remoto / pruebas)

Pantalla del navegador mostrando la página principal de BadBlue (panel o página de carga). Permite visualizar la interfaz vulnerable que será objetivo de la explotación.



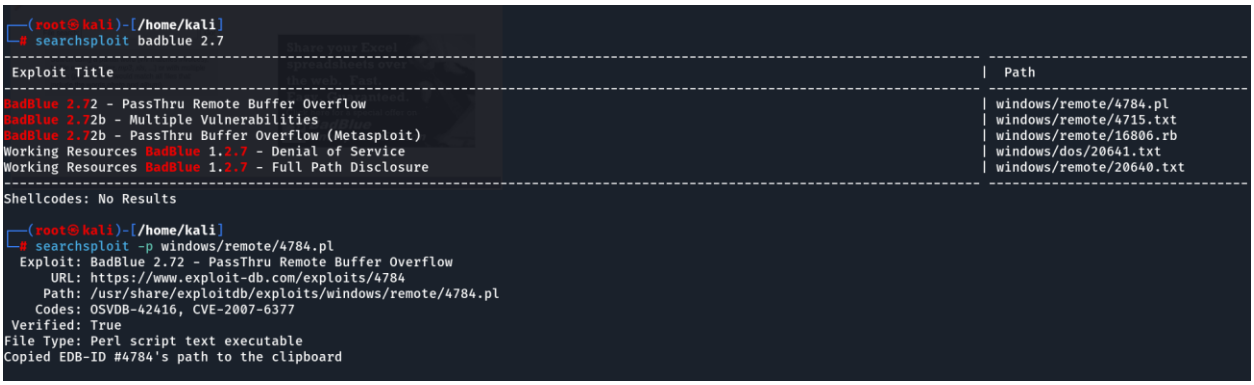
45.Interacción con la interfaz web de BadBlue

Resultado del comando curl -I http://10.0.2.7:80 mostrando HTTP/1.1 200 OK y encabezado Server: BadBlue/2.7. Esto sirve como verificación adicional de la versión exacta expuesta por el servidor.



46. Verificación del encabezado HTTP con curl

Salida de searchsploit badblue 2.7 que lista varios exploits y recursos relacionados (incluyendo el exploit 4784.pl y otros). Indica que existen exploits públicos conocidos para esa versión.



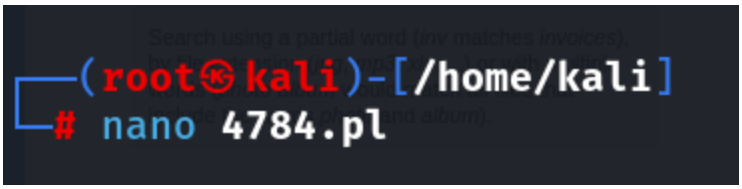
47. Búsqueda de exploits con SearchSploit

Comando cp /usr/share/exploitdb/exploits/windows/remote/4784.pl . (o similar) que copia el exploit seleccionado al directorio de trabajo del atacante para editarlo y adaptarlo. Salida de ls mostrando el archivo 4784.pl junto a otros ficheros del usuario. Confirma que el exploit fue copiado correctamente al directorio actual.

48 Copia del exploit a la carpeta de trabajo}

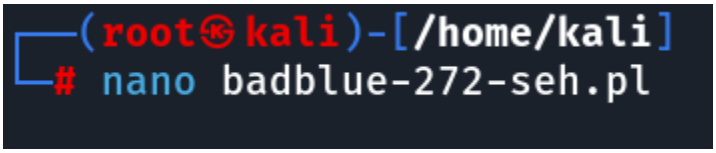
Capturas de nano 4784.pl y nano badblue-272-seh.pl indicando que el contenido del exploit se revisa o se pega en un nuevo archivo (se preparan modificadores, payloads o rutas necesarias antes de ejecutar).

Copiamos lo que aparace en nano 4784.pl



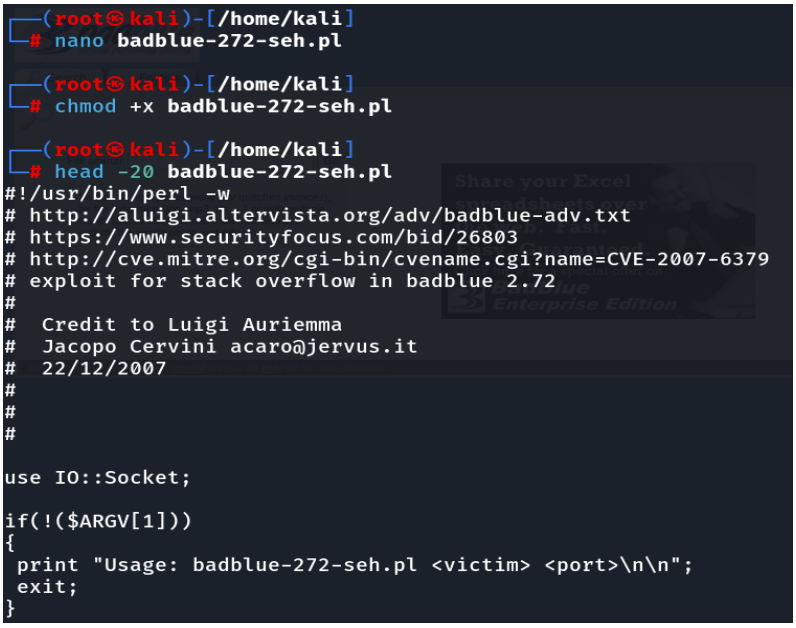
49.Edición del exploit con nano (preparación)

Lo pegamos en



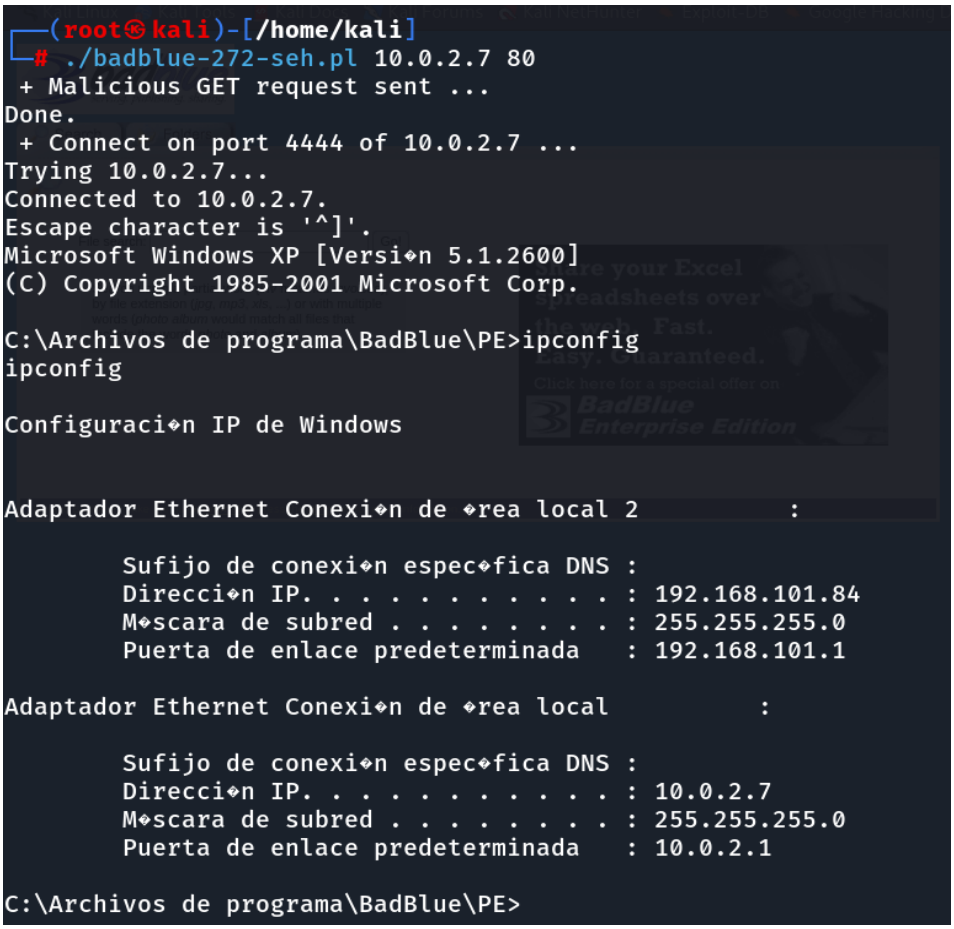
50. Edición del exploit con nano badblue-272-seh.pl

En esta etapa se abre y edita el archivo *badblue-272-seh.pl* mediante el comando nano en Kali Linux. Luego se otorgan permisos de ejecución con chmod +x. Finalmente, se visualiza el encabezado del script donde se observa la referencia al exploit de desbordamiento de pila (stack overflow) en **BadBlue 2.72**.



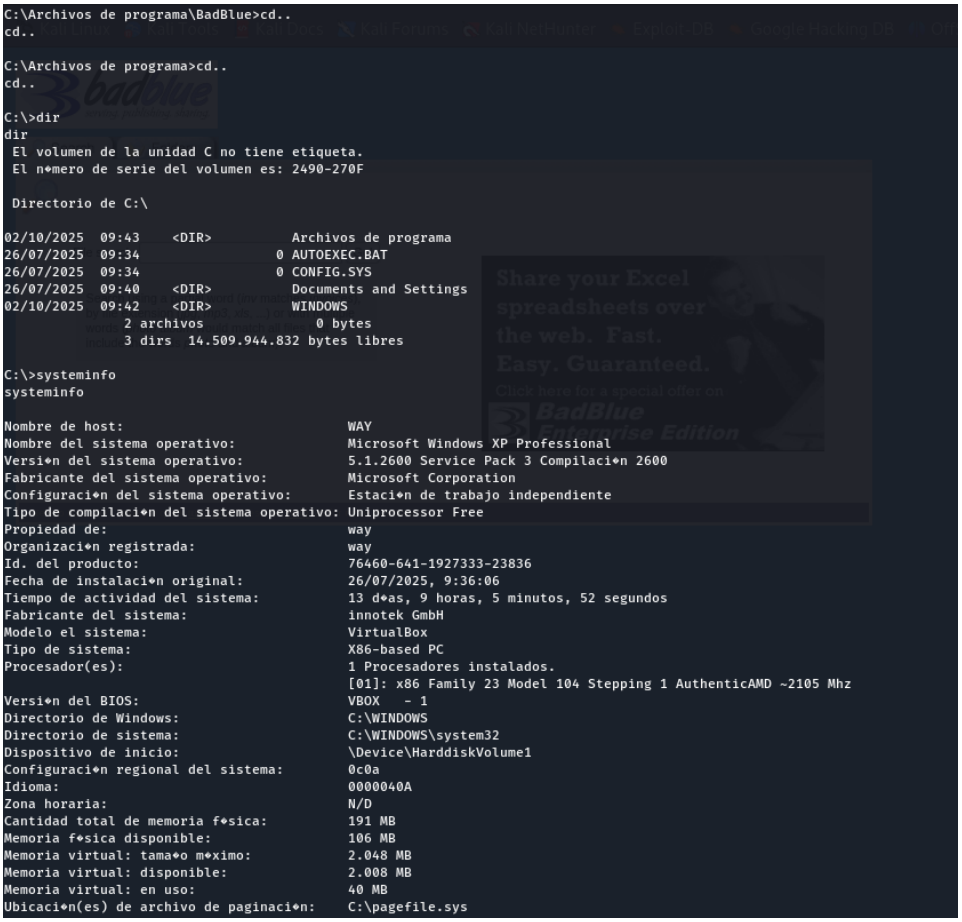
51.Creación y configuración del exploit badblue-272-seh.pl

Se ejecuta el exploit badblue-272-seh.pl apuntando a la dirección IP de la víctima (10.0.2.7) por el puerto 80. El script envía una solicitud GET maliciosa y establece una conexión reversa en el puerto 4444, obteniendo acceso remoto a la máquina Windows XP comprometida. Una vez dentro, se ejecuta el comando ipconfig para verificar la configuración de red del sistema atacado.



52.Ejecución del exploit y conexión con la víctima

Desde la sesión remota en Windows XP, se navega por el sistema de archivos y se listan los directorios del disco local (C:). Con el comando systeminfo se obtiene información detallada del sistema operativo, versión, fabricante, tipo de procesador, memoria y configuración del entorno virtualizado, confirmando el control total del sistema.



53.Exploración del sistema comprometido

Mediante los comandos net users y systeminfo, se realiza la enumeración de usuarios existentes en el equipo comprometido. Se identifican las cuentas **Administrador**, **Invitado**, **Asistente de ayuda** y **wayner_antonio_moya**, lo cual demuestra el nivel de acceso alcanzado dentro del sistema víctima.

```
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:                 106 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:      10.0.2.3
                                                 Direcciones IP
                                                 [01]: 10.0.2.7
                                           [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:      192.168.101.1
                                                 Direcciones IP
                                                 [01]: 192.168.101.84

C:\>net users
net users

Cuentas de usuario de \\WAY

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


C:\>
```

CONCLUSIÓN

El desarrollo de este informe permitió comprender de manera integral cómo interactúan los distintos componentes de un proceso de auditoría en seguridad informática. A través de la creación de entornos virtualizados y el uso de herramientas como **Camouflage**, **sha1sum** y **BadBlue**, se evidenció la importancia de la práctica en la formación de competencias en **ciberseguridad, análisis forense y pruebas de penetración**.

La instalación de controladores en Kali Linux y la configuración de carpetas compartidas demostraron la relevancia de mantener un entorno de pruebas estable, seguro y funcional. El uso de la **esteganografía** permitió visualizar técnicas de ocultamiento de información que, aunque pueden ser utilizadas de forma maliciosa, también son útiles en contextos de seguridad y cifrado de datos. Por otro lado, la **generación de hashes forenses** reforzó el conocimiento sobre los métodos de verificación de integridad, esenciales en investigaciones digitales y cadenas de custodia.

Finalmente, la **explotación controlada de la vulnerabilidad del servicio BadBlue 2.7** puso de manifiesto cómo los errores de programación o configuración pueden ser aprovechados para obtener acceso no autorizado a un sistema, resaltando la necesidad de mantener políticas de seguridad actualizadas, realizar auditorías constantes y promover la cultura de la ciberseguridad.

En conclusión, este trabajo representa un paso fundamental hacia la comprensión práctica y ética de las herramientas de seguridad, consolidando las bases necesarias para desempeñar funciones en auditoría, defensa de redes y análisis forense dentro del ámbito profesional de la ingeniería en telecomunicaciones e informática.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

REFERENCIA BIBLIOGRÁFICA

Ingeniero Rafael Sandoval