



Taskkill

## Introducción

Ante todo decir que este es mi primer manual (por lo tanto los errores y demás no me lo toméis en cuenta), con este manual no os vais a convertir en hackers ni mucho menos, este manual esta pensado para iniciaros en el mundo del hacking y sobre todo saber proteger vuestros servidores, ordenadores... de ataques, por eso en este manual se citan algunos de los ataques mas comunes, porque conociendo la forma de atacar sabremos asegurar nuestro servidor, ordenador....

En este manual e intentado explicar y poner ejemplos para que sea mas llevadero su aprendizaje, mas que un manual de técnicas hacking es un manual de conceptos y algunos conocimientos hacking para que esas personas que no saben por donde empezar lo tomen como referencia para seguir con sus conocimientos mas adelante, para que cuando estén en foros, o en Internet buscando información sobre hacking sepan y entiendan todo lo que lean con esto me refiero a que por ejemplo si están leyendo un artículo que habla sobre un ataque D.O.S que sepan y entiendan que es un ataque D.O.S y en que se basa para que a partir de ahí sigan con sus conocimientos y su aprendizaje, por que lo que esta claro es que nadie va a aprender por ti, te podrán enseñar , ayudar e incluso guiarte pero nadie lo va hacer por ti, en el mundo del hacking todos quieren o queremos ayudar pero hay que tener unos conocimientos mínimos y esos conocimientos tienes que aprenderlos tu con el día a día.

También decir que con este manual no intento formar a nadie para dar un mal uso de sus conocimientos (lammers), si no aprovecharlos pero nunca para internar molestar a otras futuras personas. Otra cosa muy importante en este mundo del hacking es nunca fastidiar a otras personas, si alguna vez encontráis alguna vulnerabilidad o un agujero de seguridad grave y lo explotáis siempre debéis informar al usuario para que corrija ese error nunca debéis aprovecharos de el para fastidiar os recomiendo que busquéis en Internet algún artículo sobre la verdadera ética de un hacker.

Bueno pues espero que os guste este manual, que le saquéis mucho provecho y por favor que me mandéis a la siguiente dirección de correo "b4t5cx@hotmail.com" vuestras opiniones sobre lo bueno y lo malo del manual os lo agradecería muchísimo.

\*No me hago responsable de de las acciones que puedan realizar las personas que lean este manual.

## Comandos Básicos

Comandos para usar desde el interprete de comandos (algunos específicos del Windows XP).

Esta NO es una lista de los comandos básicos. Nos centraremos en estos pocos, útiles en un futuro al obtener una shell remota.

**Netstat** Muestra las conexiones actuales y los puertos en escucha.

Netstat: muestra las conexiones

-a: muestra las conexiones y los puertos en escucha.

-b: muestra los ejecutables involucrados en la conexión o causantes del puerto en escucha.

-n: muestra los puertos y las conexiones en números.

-o: muestra el ID del proceso involucrado en la conexión o puerto en escucha.

\*Para mas información sobre este comando escribir en el interprete de comandos, `netstat/?`

**Bootcfg** Nos muestra la configuración del archivo boot.ini. Como ser, sistema operativo por defecto, tiempo de espera, lista, etc.

**Reg** Es una herramienta para administrar el registro, desde la consola. Nos permite consultar, exportar, modificar, copiar, comparar y más. Escribiendo, `reg` vemos la sintaxis.

**Schtasks** Le permite al Administrador, crear, borrar, consultar, modificar, ejecutar y terminar tareas programadas tanto en el sistema local, como en uno remoto.

Escribiendo `schtasks /?` vemos la lista de posibles parámetros.

**Shutdown** Nos permite apagar o reiniciar nuestra máquina. Siendo Administrador, tenemos la posibilidad de hacerlo remotamente. Al escribir `shutdown`, veremos una lista de las opciones posibles.

-Shutdown -l =Cierra la sesión del usuario

-Shutdown -s = Apaga el equipo

-Shutdown -r =Apaga y reinicia el equipo

-Shutdown -a = Anula el apagado del equipo

**Systeminfo** Vemos la configuración básica del sistema, como la versión, tipo de microprocesador, configuración de memoria, actualizaciones y muchísimas cosas mas.

**Tasklist** Nos muestra la lista de procesos que se encuentran en ejecución.

Esta lista, se puede ver de manera visual, presionando `Ctrl+Alt+Supr`, eligiendo **Administrador de Tareas** y por último la solapa de **Procesos**.

**Taskkill** Este comando nos permite terminar (matar) uno o mas procesos.

Los procesos pueden ser terminados ya sea por su Id (PID) o nombre.

\*Pid: Es el numero de proceso que esta usando cada programa en un momento determinado.

\*Para mas información sobre este comando escribimos en el interprete de comandos, `taskkill /?`

Ejemplo:

`taskkill /pid x` Donde x es el numero del proceso que queramos acabar o matar.

Hay algunos procesos que no se pueden acabar tan fácilmente como antivirus, cortafuegos... Para estos casos se fuerza el cierre del programa:

`Taskkill /f /pid x` Donde x es el numero de proceso que queramos acabar o matar.

\*Algunos comandos no funcionan en Windows XP Home Edition, los comandos ya comentados fueron probados en Windows XP Professional

# Protocolo FTP

## File Transfer Protocol

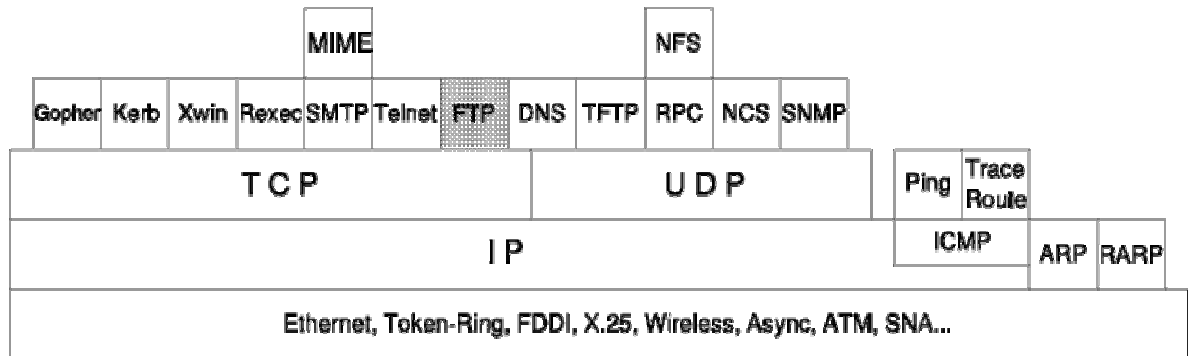


Figura: FTP

### Comandos FTP

Comandos más usuales para controlar un FTP:

- cd:** Entra en un directorio remoto.
- close:** Cierra la conexión ftp abierta.
- delete:** Borra un fichero remoto.
- dir:** Ver el contenido del directorio activo en la conexión FTP.
- get:** Bajarte un fichero desde la unidad remota.
- ls:** Listar el directorio completo del ordenador remoto.
- mkdir:** Crea directorios en el ordenador remoto.
- open:** Abre una conexión FTP con el ordenador remoto.
- put:** Envía un archivo al ordenador remoto.
- pwd:** Obtiene la dirección del directorio activo del ordenador remoto.
- recv:** Igual que Get.
- rename:** Renombra un archivo con otro nombre en el ordenador remoto.
- rmdir:** Borra un directorio en el ordenador remoto.
- status:** Obtiene diferentes señales de estado de la secuencia FTP.
- type:** Establece el tipo de transferencia que puede ser o bien ASCII (ASCII) o bien binaria (binary).
- user:** Indica el nombre de usuario o login de acceso FTP.

Windows posee un cliente de ftp por consola. Ejecutar [ftp.exe](#) en la línea de comandos.

Con la opción -? podemos ver las diferentes opciones.

Luego después de ejecutar [ftp.exe](#), con el comando help podemos ver los comandos disponibles.

### Ejecutar comandos almacenados en un archivo

FTP -s parametros.txt

El parámetro -s Carga un archivo ASCII con una lista de comandos.

### Ejemplo de comandos en un archivo .txt:

```
Open 127.0.0.1
Userprueba
Passprueba
get nc.exe
Put kill.exe
Close
Quit
```

## Protocolo TFTP

TFTP: Trivial file transfer protocol, es un protocolo extremadamente trivial para la transferencia de ficheros. Se implementa sobre la capa UDP (User Datagram Protocol) y carece de la mayoría de las características de ftp.

Para utilizar el servicio TFTP desde nuestro intérprete de comandos escribimos TFTP.exe:

Aquí tenemos algunos comandos para su uso:

-Get: Obtener

-Put: Enviar

-La opción -i siempre hay que especificarla.

### Ejemplo:

En este ejemplo vamos a bajar el archivo hola.exe que esta ubicado en C: Estamos situados en una red de área local con dos ordenadores, atacante: 192.168.1.2 y servidor: 192.168.1.13

1-Ejecutamos el interprete de comandos en este caso cmd.exe (MS-dos)

2-Ponemos tftp -i (hay que especificarla siempre) IP (en este caso la del servidor) get (para descargar el archivo) y el archivo en este caso hola.exe.

TFTP -i 192.168.1.13 get hola.exe

\*Para hacer este ejercicio hay que tener habilitado el protocolo UDP ya que el servidor tftp trabaja bajo el protocolo UDP, deshabilitar cortafuegos (en caso de que hubiese alguno) y tener paciencia ya que falla mucho.

Se recomienda tener un servidor de Tftp es un pequeño programa su nombre es tftpd32.exe. Con este método conseguimos bajar o subir archivos sin ningún tipo de autenticación (Contraseñas ni usuarios) pero falla mucho, la mayoría de los errores los provoca la terminación de la conexión (falta fiabilidad). Si un paquete se pierde en la red, se produce "time out", tras el que se efectuara la retransmisión del ultimo paquete. Posee un bug grave que se llama Síndrome del aprendiz brujo.

## Proxies

UN Proxy funciona haciendo una conexión intermedia entre tu ordenador y el destino al que quieres acceder. Es decir:

Si quieres conectarte a [www.microsoft.com](http://www.microsoft.com) tu máquina hace la solicitud a [www.microsoft.com](http://www.microsoft.com) pero si usas un Proxy en vez de hacer la solicitud a [www.microsoft.com](http://www.microsoft.com) se la haces al Proxy y este se la hace a

[www.microsoft.com](http://www.microsoft.com) Así quedara marcada la IP del Proxy en el sistema donde se aloja [www.microsoft.com](http://www.microsoft.com) y no la tuya, ya que vos nunca estableciste una conexión directa con [www.microsoft.com](http://www.microsoft.com) sino con el Proxy y éste fue quien la hizo con [www.microsoft.com](http://www.microsoft.com)

Existen muchos tipos de proxies, transparentes, anónimos o totalmente anónimos. Los transparentes para lo que sea seguridad informática o hacking no sirven. Tienen que ser anónimos o totalmente anónimos. Los proxies anónimos o totalmente anónimos ocultan nuestra IP. La diferencia entre estos dos, radica en que los totalmente anónimos, ocultan el hecho de que se está usando un Proxy.

-El uptime de un Proxy significa cuanto tiempo podemos estar conectados a el.

-“Average response Time (ns)”, es el tiempo de respuesta del Proxy.

#### **Direcciones con proxies:**

<http://www.samair.ru/proxy/socks.htm>

<http://www.atomintersoft.com/products/alive-proxy/proxy-list/high-anonymity/>

<http://www.atomintersoft.com/products/alive-proxy/socks4-list/>

<http://www.multiproxy.org/cgi-bin/search-proxy.pl>

Existen varios tipos de proxies, siendo los más usuales los HTTP Proxies que en teoría solo sirven para navegar por Internet, aunque algunos poseen soporte para ftp.

Los más completos son los SOCKS (v4 y v5 y se diferencian que el v5 soporta autenticación y el v4 no), que permiten casi cualquier protocolo con lo que son multipropósito. Estos son los proxies que están instalados en el puerto 1080 por defecto.

#### **Es posible encadenar proxies**

Tu PC --> Proxy 1 --> Proxy 2 --> ... .. --> Víctima

Esto puede hacerse con programas tales como el SOCKSCHAIN.

## **Como funciona el anonimato en un proxy HTTP.**

Un cliente envía una solicitud (el archivo que requiere) y el servidor envía la respuesta (archivo solicitado). El cliente envía información adicional sobre el mismo: la versión y nombre del sistema operativo, configuración del navegador incluyendo el nombre y la versión, etc. Esta información puede ser necesaria para que el servidor sepa que pagina enviar al cliente.

Información que el navegador envía al servidor Web:

- Nombre y versión del sistema operativo.
- Nombre y versión del navegador.
- configuración del navegador (resolución de pantalla, lenguaje preferido, java / javascript support, ...)
- Dirección IP del cliente
- Otra información

La parte mas importante de ésta información (y que el servidor no necesita) es la información sobre la dirección IP. Es posible para el servidor, saber toda esta información obtenida de la IP del cliente:

- El país de donde proviene
- La ciudad
- El proveedor de Internet y el mail
- La dirección física

La información transmitida por el cliente a un servidor es transmitida como variables de entorno.

Estas son las variables de entorno que nos interesan:

REMOTE\_ADDR – dirección IP del cliente

HTTP\_VIA – si no está vacía, un Proxy esta siendo usado. El valor es una dirección de un servidor Proxy. Esta variable es añadida por el servidor Proxy si usas uno.

HTTP\_X\_FORWARDED\_FOR – si no está vacía, un Proxy esta siendo usado. El valor es la dirección IP del cliente, esta variable es agregada por el Proxy si usas uno.

HTTP\_ACCEPT\_LANGUAGE – que lenguaje usa el navegador (es decir, que lenguaje debe ser mostrado)

HTTP\_USER\_AGENT – nombre del navegador y su versión (Ej.: MSIE 5.5) y el sistema operativo (Ej.: Windows 98).

HTTP\_HOST – es el nombre del servidor Web.

Esta es una pequeña parte de las variables de entorno. Existen muchas mas (DOCUMENT\_ROOT, HTTP\_ACCEPT\_ENCODING, HTTP\_CACHE\_CONTROL, HTTP\_CONNECTION, SERVER\_ADDR, SERVER\_SOFTWARE, SERVER\_PROTOCOL,...).

Estos son ejemplos de valores de variables:

```
REMOTE_ADDR = 194.85.1.1
HTTP_ACCEPT_LANGUAGE = ar
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
HTTP_HOST = www.google.com
HTTP_VIA = 194.85.1.1 (Squid/2.4.STABLE7)
HTTP_X_FORWARDED_FOR = 194.115.5.5
```

Si un servidor Proxy no esta siendo usado, las variables contienen estos valores:

```
REMOTE_ADDR = your IP
HTTP_VIA = not determined
HTTP_X_FORWARDED_FOR = not determined
```

De acuerdo a como los valores de dichas variables son ocultados, los proxies se clasifican en:

### ***Proxies Transparentes***

No esconden la información sobre tu IP:

```
REMOTE_ADDR = proxy IP
HTTP_VIA = proxy IP
HTTP_X_FORWARDED_FOR = your IP
```

Estos proxies no mejoran tu anonimato en Internet. El propósito de éstos es el de cache o el de brindar acceso a Internet a varias computadoras, etc.

### **Proxies Anónimos**

Son todos los proxies que ocultan la IP del cliente.

#### *Proxies Anónimos Simples*

Estos proxies no ocultan el hecho de que se esta usando un Proxy, aunque remplazan tu IP por la de ellos:

```
REMOTE_ADDR = proxy IP
HTTP_VIA = proxy IP
HTTP_X_FORWARDED_FOR = proxy IP
```

#### **Proxies de Alto anonimato**

O "high anonymity Proxy", esconden el hecho de que se esta usando un Proxy:

```
REMOTE_ADDR = proxy IP
HTTP_VIA = not determined
HTTP_X_FORWARDED_FOR = not determined
```

## **Troyanos, Backdoors, Keyloggers y Worms**

### **Troyanos**

Un troyano no es directamente un virus, dado que no se reproducen. Son programas ejecutables que son ingresados a un sistema por un usuario malicioso de una forma encubierta, como un programa amistoso, gráficos, juegos, etc. De esta manera, al ser ejecutados, realizan acciones que el usuario no desea y que fueron programas por quien envió el troyano.

### **Backdoors**

Un backdoor es un programa que se introduce en el ordenador de manera encubierta, aparentando ser inofensivo. Una vez ejecutado, establece una "puerta trasera" a través de la cual es posible controlar el ordenador afectado.

### **Keyloggers**

Son programas, que generalmente corren escondidos en la PC y que registran cada tecla que es presionada en tu teclado. Actualmente muchos tienen opciones como sacar "screenshots" cada X minutos, ver los programas que se encuentran corriendo, ver los programas que tiene el foco, URLs que son visitadas, etc. Es posible programar algunos keyloggers para que envíen toda ésta información a un email especificado.

### **Worms (Gusanos)**

Son programas que se replican a si mismos de sistema en sistema sin utilizar un archivo para hacerlo, se parece a los virus en que su principal función es reproducirse pero por el contrario de cómo lo hacen los virus en lugar de copiarse dentro de otros archivos, crean nuevas copias de si mismo para replicarse.



## Defacement

Técnica hacking que consiste en un cambio de cara a una pagina Web, la persona que utiliza esta técnica cambia o modifica en index de una pagina Web, sitios Web hacheados:

<http://www.e-literatura.com>  
<http://www.portalrecursos.com>

Para buscar mas paginas Web hacheadas en un buscador probar a poner esto:  
"intitle: "Hacked by "???"

## Fuerza Bruta HTTP – FTP – POP3 y Diccionarios

Consiste en probar constantemente nombres de usuarios y contraseñas, hasta coincidir una cuenta. Este método en la teoría asegura un éxito del 100% en la búsqueda (ya que probamos todas las posibilidades), pero tiene un gran inconveniente, el tiempo. Como salta a la vista, probar todas y cada una de las posibilidades es altamente costoso en tiempo y de hecho este método tiene sentido en caso de realizarlo localmente en la maquina contra una clave encriptada (utilizando aplicaciones como el john the ripper).

Contra un host remoto este método no es nada recomendable, se suele considerar mucho más el ataque con diccionario. El diccionario consiste en un archivo de texto plano (.txt) donde residen todas las palabras una debajo de la otra. Cuando la fuerza bruta está apoyada en un diccionario, comprobará todos los passwords que se tengan en dicho diccionario. Estos intentos pueden hacerse simultáneos (por ejemplo 5 a la vez, y si la aplicación remota lo permite) o de a uno en uno.

No se utiliza la fuerza bruta convencional para ataques remotos por el tiempo que llevaría probar todas las combinaciones, Ej.: Probar todas las combinaciones entre 3 y 10 caracteres a 500 intentos por minuto nos llevaría 14309817 años con 280 días.

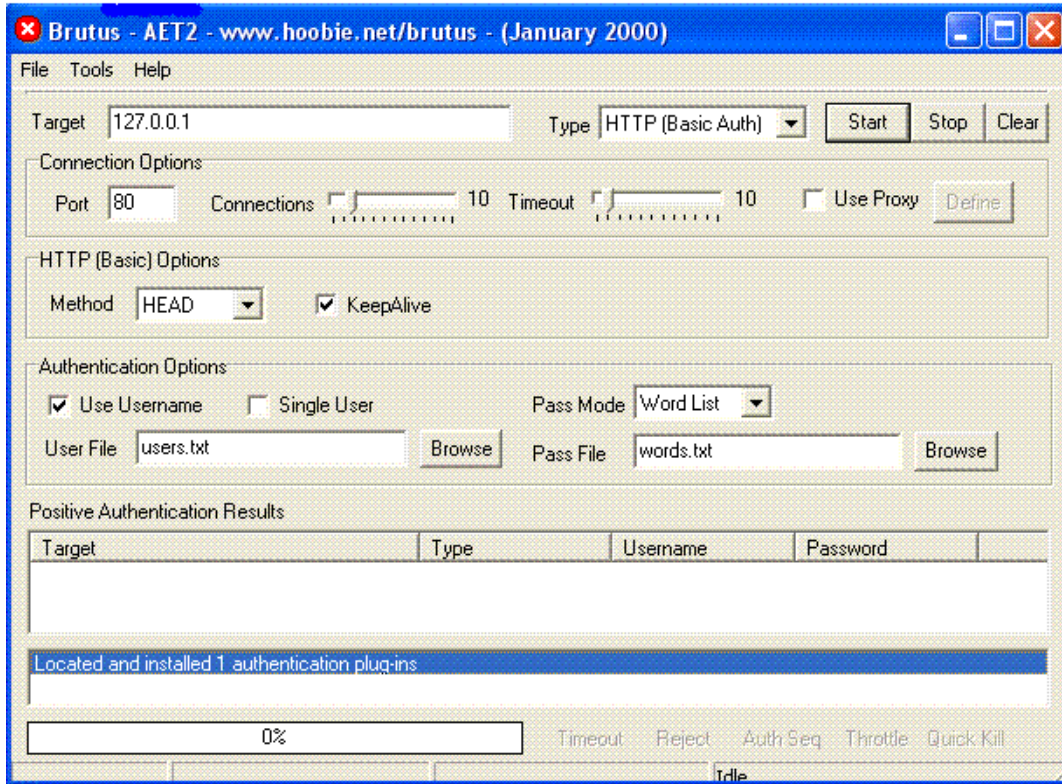
A diferencia del diccionario utilizado para craking realizado con el Jhon para craquear un archivo con contraseñas en la PC (archivos de varios megas, con palabras en diferentes idiomas, de varios tipos y palabras de todo tipo), el diccionario para realizar fuerza bruta ftp, http, pop3, etc, debe ser compacto, por ejemplo, no mayor a 60 o 70 Kb. Deben elegirse las palabras que éste diccionario incluirá y confeccionarlo con las palabras con más probabilidades de coincidir. **Agrega** palabras y ve modificándolo hasta que poseas un buen diccionario de reducido tamaño y gran calidad.

También existe el problema de que con la fuerza bruta se genera una gran cantidad de log. Esto tenlo en cuenta.

**Herramienta: wwwhack** No permite la utilización de Proxy. Posee una útil opción para armar diccionarios, la cual consiste en suprimir palabras repetidas. Es muy inestable.

### **Herramienta: Brutus**

Permite la utilización de proxies. Ataque por diccionario o fuerza bruta a FTPs, http, formularios, POP3 y SMTP.



Esta es la apariencia de Brutus

## Scanner de Vulnerabilidades

### Retina

Es un scanner de vulnerabilidades de la empresa eEye. Ciertamente es una muy buena herramienta de AUDITORIA de redes. Tiene funciones para imprimir y personalizar reportes, Live Update, políticas de uso ampliamente configurables y más. Esta herramienta es de gran importancia en el mundo del hacking, siendo un muy buen scanner. PERO el Retina no se concibió para hacking, sino para auditoria. Siendo completo en muchos aspectos referentes a la auditoria, es evidente que se queda corto como herramienta de Hacking. Debe utilizarse además, otro scanner, mas orientado a lo que es Hacking. Al ser orientado a la auditoria, no brinda cierta información muy necesaria (que otros si lo hacen) utilizada para el hack.

### X-Scan

X-Scan es un analizador de vulnerabilidades de todo tipo de redes para rangos específicos de IP o para analizar un único ordenador. Soporta plug-ins. Se proporcionan por separado las interfaces graficas y de línea de comandos, pudiéndose ejecutar tanto desde la línea de comandos como desde un entorno Windows amigable haciendo un doble clic sobre el icono de la navaja suiza en Windows. No necesita instalación.

Se pueden analizar los siguientes elementos: tipo de servicio, tipo de sistema operativo y versión basado en pila TCP/IP (como lo hace nmap), debilidad en los pares usuario/contraseña de los protocolos; y, como novedad, scripts de ataque Nessus. Se proporcionan las descripciones y las soluciones correspondientes para las vulnerabilidades conocidas.

No necesita instalación.

### **Algunas funciones:**

Chequea si el host objetivo está activo  
Chequea el sistema operativo objetivo mediante NETBIOS y protocolo SNMP  
Analiza el estado de los puertos más comunes  
Analiza contraseñas débiles en FTP  
Chequea permisos de escritura anónimos y públicos en servidor FTP  
Analiza contraseñas débiles en servidor POP3;  
Análisis vulnerabilidad en servidor SMTP  
Analiza contraseñas débiles en servidor en SQL Server  
Analiza contraseñas débiles en servidor NT  
Análisis de vulnerabilidades CGI  
Análisis de vulnerabilidades IIS  
Scripts de ataque Nessus

## **Investigación del Sistema e Identificación de Vulnerabilidades**

Recabar toda la información posible.  
Que sistema Operativo usa, que versión y en que idioma.  
Puertos, Servicios y aplicaciones. (Con un escáner de puertos y con uno de vulnerabilidades)  
Determina la aplicación que corre ese servicio y versión. Busca por posibles vulnerabilidades en las aplicaciones que has encontrado. (Con un escáner de vulnerabilidades)  
Busca en Internet por vulnerabilidades (por ejemplo en [www.securityfocus.com](http://www.securityfocus.com) ) en las versiones de las aplicaciones que el servidor esta corriendo. Revisa e investiga la documentación para explotarlas, tan importante como la exitosa explotación de la vulnerabilidad, es saber que se esta haciendo y como. Trata de, en lo posible, ocultar o anonimizar tu ataque.

Estos son algunos puertos muy comunes:

SMTP	25
Pop	110
Ftp	21
Http	80
Tftp	69
Telnet	23

Los puertos van desde 1 al 65525.

## **Pasos a seguir para Penetración a un sistema, Penetración testing o Hacking**

### **1Paso**

Investigación del sistema: Sistema operativo que utiliza, versión del S.O que utiliza e idioma en el que lo utiliza

### **2Paso**

Identificación de puertos y servicios: Puertos abiertos y aplicaciones que corren, junto a sus versiones

### **3Paso**

Encontrar vulnerabilidades: Vulnerabilidades http, ftp, RPC... y configuración del sistema.

### **4Paso**

Una vez que tenemos todo esa información: Deberemos buscar información sobre la vulnerabilidad (una buena página es [www.securityfocus.com](http://www.securityfocus.com))

## 5Paso

Una vez que tenemos la información procederemos a explotarla, ya sea con exploit o de alguna otra manera depende de la vulnerabilidad

\*RPC=Llamada a procedimiento remoto. El blaster explotaba una vulnerabilidad del RPC

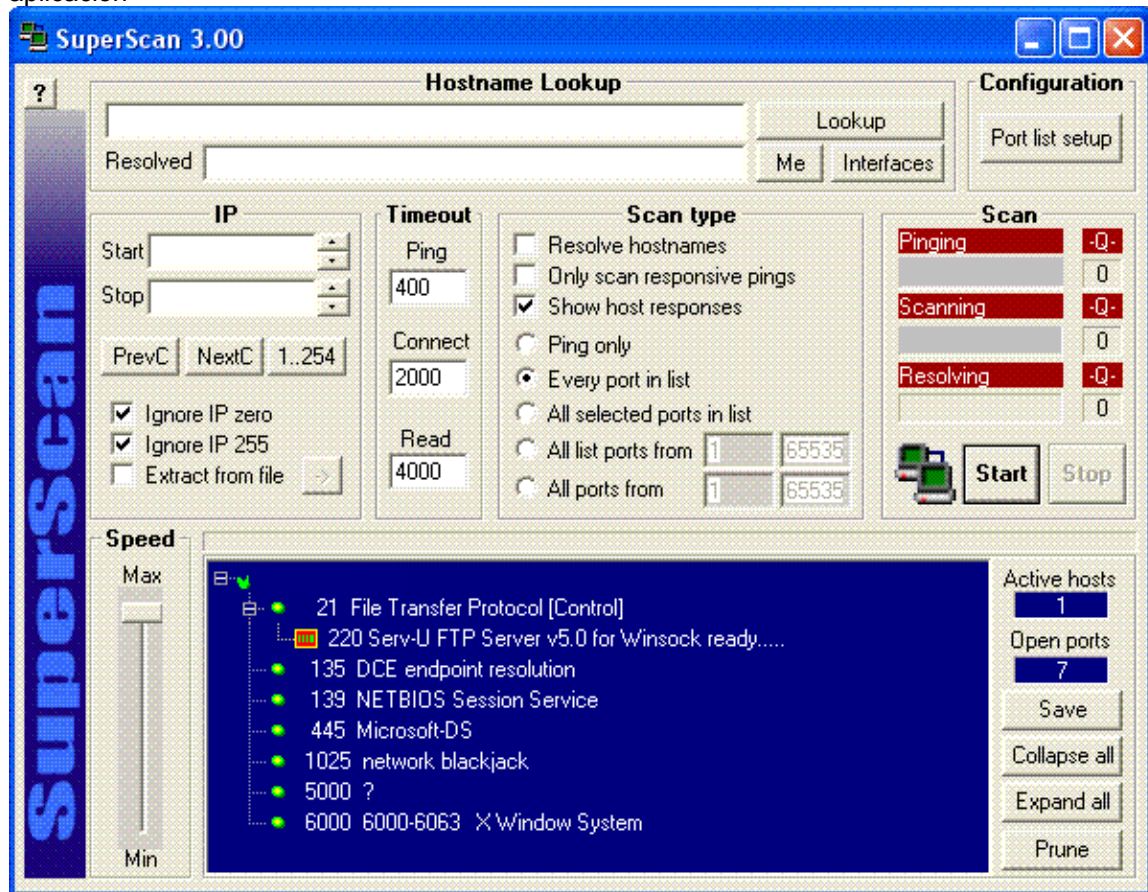
\*IDS= Sistema de detención de intrusos.

Scaneo de puertos e identificación de Servicios

Algunos conceptos que hacen falta saber:

-Banner: Cartel o mensaje. Lo utilizan algunos programas y en el dicen su versión e información del programa

-Banner de respuesta= Al hacer una conexión, el servidor responde con un banner a veces identifica la aplicación



Fijaos, en el puerto 21 donde pone "21 File Transfer Protocol (control)", pues justamente debajo esta el banner de respuesta del puerto 21 donde pone "220 Serv-U FTP Server v5.0 for Winsock ready..."

-IIS= Internet information Server, servidor web de Microsoft.

-Windows NT= Utiliza IIS 3.0/4.0

-Windows 2000= Utiliza IIS 5.0

-Windows XP=Utiliza IIS 5.1

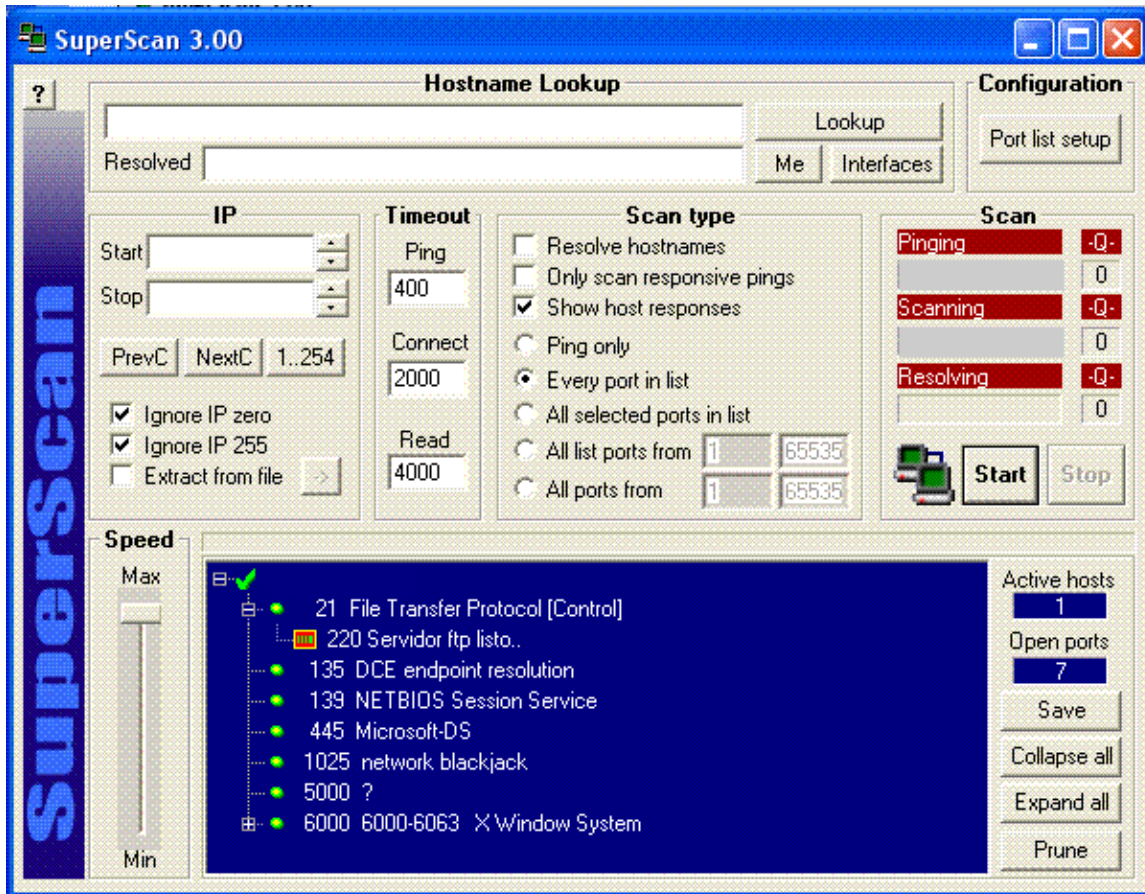
-Windows 2003=Utiliza IIS 6.0.

-SSH=Secure shell, característico de Linux

\*Tanto IIS Y SSH os ayudaran para diferenciar Sistemas operativos y sus respectivas versiones.

\*También hay que decir que hay que tener mucha atención con los “false positives” (falsos positivos), algunos banners se pueden configurar manualmente para engañar al atacante.

Ej.: Si en un sistema Win Xp hay un servidor de ftp llamado Serv-U 5.0, por defecto el banner viene con el nombre del programa pero nosotros lo podemos modifica y poner”Servidor ftp listo” de esta manera ya estaríamos engañando al atacante.



Este es ejemplo que os comentaba fijaos en el banner ya no pone “220 Serv-U FTP Server v5.0 for Winsock ready...” ahora pone “220 Servidor ftp listo”

Ejemplo de servicios y aplicaciones

Servidor ftp Serv-U 5.0 ¿Cuál es el servicio y cual la aplicación?

Solución: El servicio es el ftp y la aplicación es el servidor de ftp serv-U 5.0



## ¿Qué hacer cuando se tiene una shell de un sistema?

Al obtener una shell y con permisos de administrador, manejamos todo el host. Una shell puede utilizarse para encubrir ataques a otros host entre otras, al obtenerse la shell se debe investigar el sistema por completo:

- Revisar directorios
- Buscar archivos que contengan password

Algunos archivos que contienen password y usuarios (encriptados):

Ws\_ftp.ini (cuteftp), smdata.dat (cuentas de correo), user.cif (pcanywhere), eudora.ini, wcx\_ftp.ini, servudaemon.ini, accnts.ini, ftplist.txt, etc...

-A veces podemos encontrar cosas interesantes en un archivo como importante.xls o importante.doc, cuentas.txt etc....

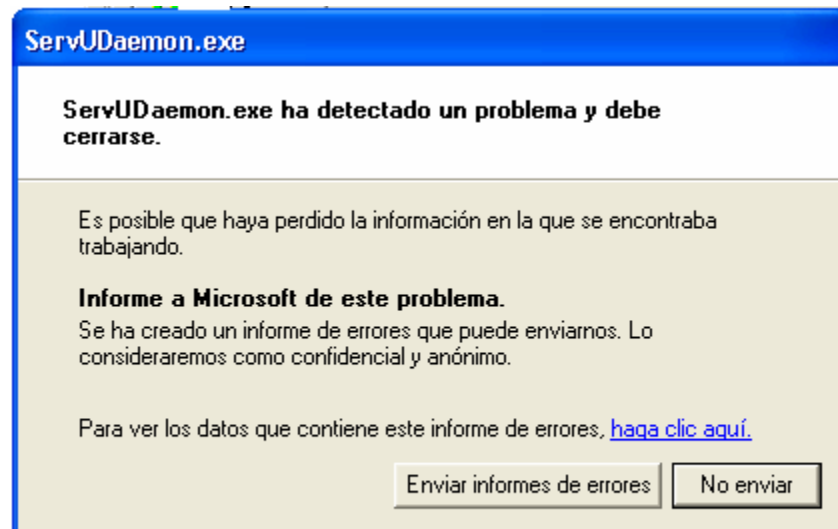
- Buscar la existencia de otras unidades
- Buscar la existencia de otras maquinas en red.

## Definiciones

### D.O.S (Denegación de servicio)

D.O.S Denial of Service (Denegación de Servicio), consiste en impedir el acceso de usuarios legítimos a un servicio o recurso, mediante un ataque que se puede restringir el acceso a las personas al servidor por lo tanto evitar que realicen su trabajo.

Pueden producirse **explotando una vulnerabilidad del sistema** o mediante flooding, email bombing, synflood, etc.



Esta foto muestra lo que generaría un ataque D.O.S a un servidor de ftp Serv-U v5.0.

## Email Bombing

En un ataque de email se envían muchos mensajes idénticos a una dirección, produciendo el llenado del espacio disponible para dicha cuenta de email. En las cuentas que solo podían revisarse mediante POP, había que bajarse todos esos mails para poder vaciar la cuenta.

¿Qué daños causa esto? Llenaría la cuenta de correo, además si la cuenta no es webmail y solo pop tendría que bajar todos esos mensajes al disco duro para poder borrarlos.

## Abuso del FTP anónimo

Si un servidor FTP anónimo tiene un área que pueda ser escrita puede ser abusada para un ataque de negación del servicio. Obviamente el objeto sería llenar el disco duro. Muchas veces el espacio de HD para la cuenta anónima está definido.

## Flooding

Enviar algo repetidamente para saturar el servidor.

## Ping

El comando ping se utiliza generalmente para testear aspectos de la red, como comprobar que un sistema está encendido y conectado; esto se consigue enviando a dicha máquina paquetes ICMP (de tipo ECHO/SMALL>\_REQUEST), tramas que causarán que el núcleo del sistema remoto responda con paquetes ICMP, pero esta vez de tipo ECHO/SMALL>\_RESPONSE. Al recibirlos, se asume que la máquina está encendida:

## Ping Flooding

Es una técnica de DoS. Se refiere al envío de un número inusual y elevado de paquetes ICMP de "requisición de eco" ("ping"), buscando saturar el dispositivo atacado. Este método tiene un gran efecto en el sistema atacado. Si te están haciendo esto desde un host con mayor ancho de banda que el de tu máquina, serás incapaz de enviar nada a la red. Puede contrarrestarse con un firewall configurado para no recibir o recibir en cantidades pequeñas los paquetes icmp.

## Ping de la Muerte

Antiguamente TCP/IP en Windows 95 no soportaba paquetes mayores a 64400 bytes. De esa manera el sistema se tornaba vulnerable a un simple comando ping: ping -t -l 65500 <IP de la víctima>. Este comando se conoce como ping de la muerte.) La opción -t indica que envíe ininterrumpidamente paquetes. Este comando causaba que el sistema operativo se colgara o reiniciara.

Para detener a un sistema desde una máquina corriendo Windows 95 simplemente ejecuta:

**Ping** -t -l 65510 prueba.com

Y el sistema se detendrá o se re-iniciará.

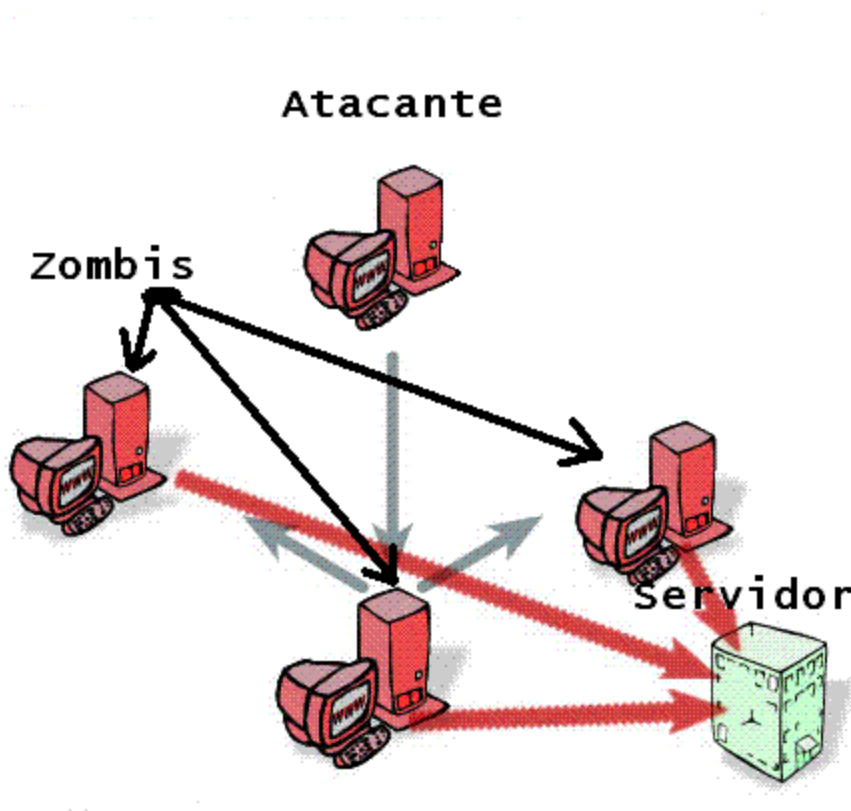
## DDoS

DDoS significa Distributed Denial of Service (Denegación de servicios distribuida). Un DDoS involucra a muchos ordenadores (mientras más mejor). Se realiza instalando un software específico para lanzar ataques o hacerlo manualmente (deberíamos acceder a cada ordenador y decirles uno a uno que debe hacer). Lo mejor desde el punto de vista del atacante es usar un software.

De esta forma, lanza el ataque masificado controlándolo todo desde un ordenador.

Las maquinas utilizadas para cometer estos ataques se llaman zombis, y suelen ser PCs de usuarios comunes, infectadas con un virus por el cual el hacker controla a esas Pcs (convirtiéndolas en zombis). Son ataques muy elaborados y difíciles de llevar a cabo. Grandes empresas se han sido victimas de este tipo de ataques, como cnn.com, ebay.com, whitehouse, etc., utilizando un cierto número de zombis. (1000, 3000, 4000)

Las consecuencias suelen ser el ahogo del ancho de banda. Siempre se pretende denegar algún recurso.



Aquí te dejo unas noticias sobre ataques de DDoS. Léela para tener una mayor noción este tipo de ataques:

<http://www.noticiasdot.com/publicaciones/2004/0704/2907/noticias290704/noticias290704-8.htm>

<http://www.aclantis.com/article2600.html>

<http://www.belt.es/noticias/2004/febrero/04/mydoom.htm>



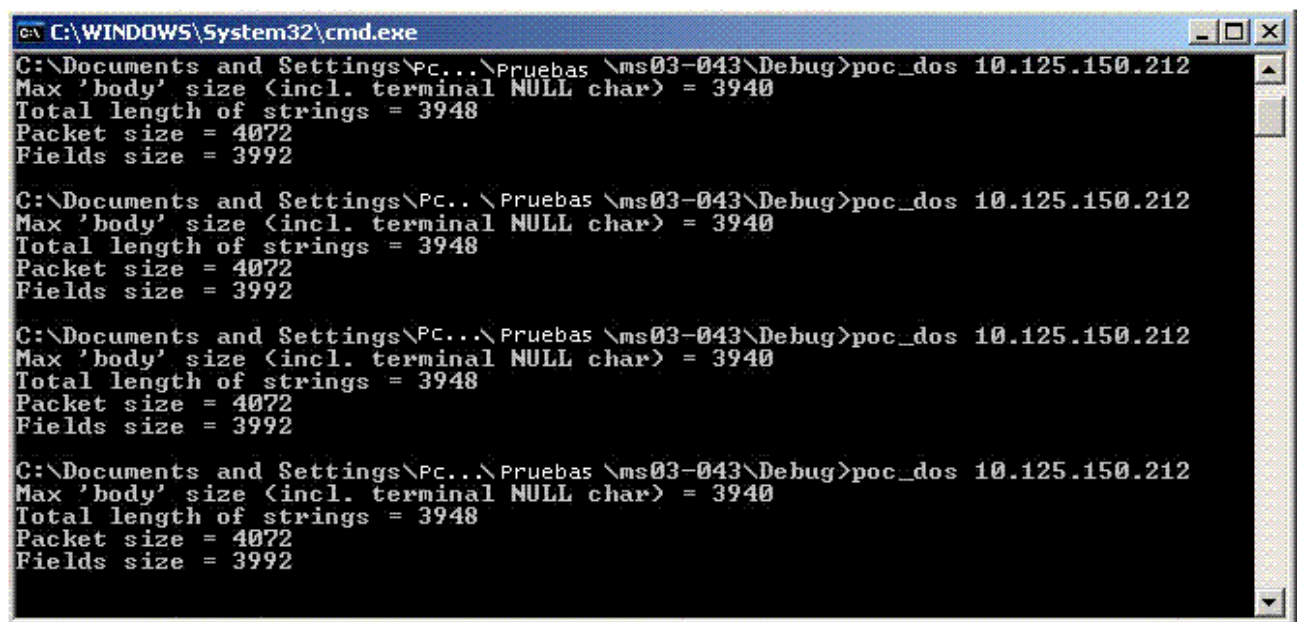
## Exploit

Son trozos de código o programas de poco tamaño que explotan alguna vulnerabilidad del sistema pueden producir un D.O.S o abrir una puerta que posibilite la entrada al sistema. Los exploit suelen estar escritos en C, C++ o Perl, algunos tienen interfaces graficas y otros se utilizan desde el intérprete de comandos.

Los exploits se pueden conseguir en Internet pero la mayoría por no decir todos no están compiladas, quiero decir que puedes encontrar su código de fuente y luego hay que compilarlos y crear el ejecutable.

¿Una vez que tienes el ejecutable de exploit como se utiliza?

Si es bajo el intérprete de comandos tienes que parametrizarlo:



```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\PC...\Pruebas\ms03-043\Debug>poc_dos 10.125.150.212
Max 'body' size (incl. terminal NULL char) = 3940
Total length of strings = 3948
Packet size = 4072
Fields size = 3992

C:\Documents and Settings\PC...\Pruebas\ms03-043\Debug>poc_dos 10.125.150.212
Max 'body' size (incl. terminal NULL char) = 3940
Total length of strings = 3948
Packet size = 4072
Fields size = 3992

C:\Documents and Settings\PC...\Pruebas\ms03-043\Debug>poc_dos 10.125.150.212
Max 'body' size (incl. terminal NULL char) = 3940
Total length of strings = 3948
Packet size = 4072
Fields size = 3992

C:\Documents and Settings\PC...\Pruebas\ms03-043\Debug>poc_dos 10.125.150.212
Max 'body' size (incl. terminal NULL char) = 3940
Total length of strings = 3948
Packet size = 4072
Fields size = 3992
```

## Buffer overflow

Es un revasamiento del buffer del sistema. Un ejemplo valido pero muy tonto es el de querer meter 1 litro de agua en un vaso en el cual solo caben 40cl de agua. Llegaría un momento en el que el agua se desbordaría (overflow) y el vaso sería el buffer.

## **RPC**

Llamada a procedimiento remoto. El blaster explotaba una vulnerabilidad del RPC

## **IDS**

Sistema de detención de intrusos

## **Banner**

Cartel o mensaje, lo utilizan algunos programas y en el dicen su versión e información del programa.

## **Banner de respuesta**

Al hacer una conexión, el servidor responde con un banner a veces identifica la aplicación

## **IIS**

Internet Information Server, servidor Web de Microsoft

## **SSH**

Secure shell, característico de sistemas Linux

# **Herramientas**

### **Para escanear puertos y servicios:**

- SuperScan (esta muy bien para aprender)
- X-Scan
- Y herramientas de Eye for ID para vulnerabilidades

### **Para descifrar algoritmos**

- Mdcrack (algoritmos, md5, md4, ntlm1, hashes)
- John the ripper (algoritmos des)

### **Ataque por diccionario o fuerza bruta**

- Brutrus AET 2.0

### **Snnifers**

- Cain v2.5

### **Gestor ftp**

- Total commander 5.51

### **Navegador de Internet**

- Mozilla Firefox

### **Keyloggers**

- Ghost keyloggers

### **Control remoto**

- Radmin
- Vnc

### **Servidor tftp**

- TFTPD 32

Y sobre todo <http://www.google.com>, ese será vuestro gran aliado, si lo que buscáis no lo encontráis en google rezar para encontrarlo (también hay que saber buscar y saber lo que se busca)

## Consejos

- Siempre que tengas duda de cómo se explota una vulnerabilidad, instala la aplicación en tu PC y prueba explotar la vulnerabilidad en dicha aplicación instalada en tu PC, es decir localmente.
- El escáner de vulnerabilidades X-Scan es el más apropiado para investigar cosas nuevas y aprender a explotar las vulnerabilidades. Ten en cuenta que suele dar bastantes falsos positivos. Practica escaneando muchos host, y observando que vulnerabilidades que encuentras. Investiga como poder explotar las vulnerabilidades ésas. Existen muchas extremadamente fáciles de explotar.
- Te recomiendo fuertemente que te registres las mailing list de [www.securityfocus.com](http://www.securityfocus.com) más precisamente en la mailing de Penetration-Testing. Es interesantísima y se aprende muchísimo. Ten en cuenta que es una de las más grandes que existen y recibes muchos mails diarios.