

Compilacion e interpretacion de Exploits escritos en:

PHP, Perl, Phyton, C y C++

## Conceptos Primarios.

¿Que es un exploit? En la red este termino se confunde masivamente con la palabra xexploit la cual existen entre estas dos unas grandes diferencias. Un exploit es el usado, como hace referencia, para explotar una vulnerabilidad ya sea a nivel software o web. Un xexploit es el usado eventualmente para robar cuentas ejerciendo la técnica de phishing, engañando a la victima con un envío de xexploit, para que ingrese a una web falsa he ingrese su nick y contraseña y asi ser capturada por el atacante.

Ya entendiendo este básico concepto de exploit, se puede decir que uno de estos podría estar escrito en distintos códigos de programación, los cuales podrían ser php, Python, Perl, c y c++, paso siguiente es enseñarle como diferenciarlos:

Todo software o en este caso un exploit escrito en perl comienza con: **#!/usr/bin/perl**

Todo software o en este caso un exploit escrito en Python comienza con: **#!/usr/bin/env python**

Todo software o en este caso un exploit escrito en php comienza con: **#!/usr/bin/php**

En el caso de c y c++, al comienzo ni al final del código se hace referencia a que esta escrito en dicho código de programación, quizás se pueda reconocerlo si se hace algún include de librerías para el exploit, pero este tema no describiré.

Todo exploit se debe compilar o ser interpretado para poder hacer que funcione de manera correcta. No solo existe una manera para compilarlos, sino que existen varias, aquí al menos explicare una para cada código de programación y para poder llevarlo a cabo *no* habrá necesidad de saber programar en alguno de estos.

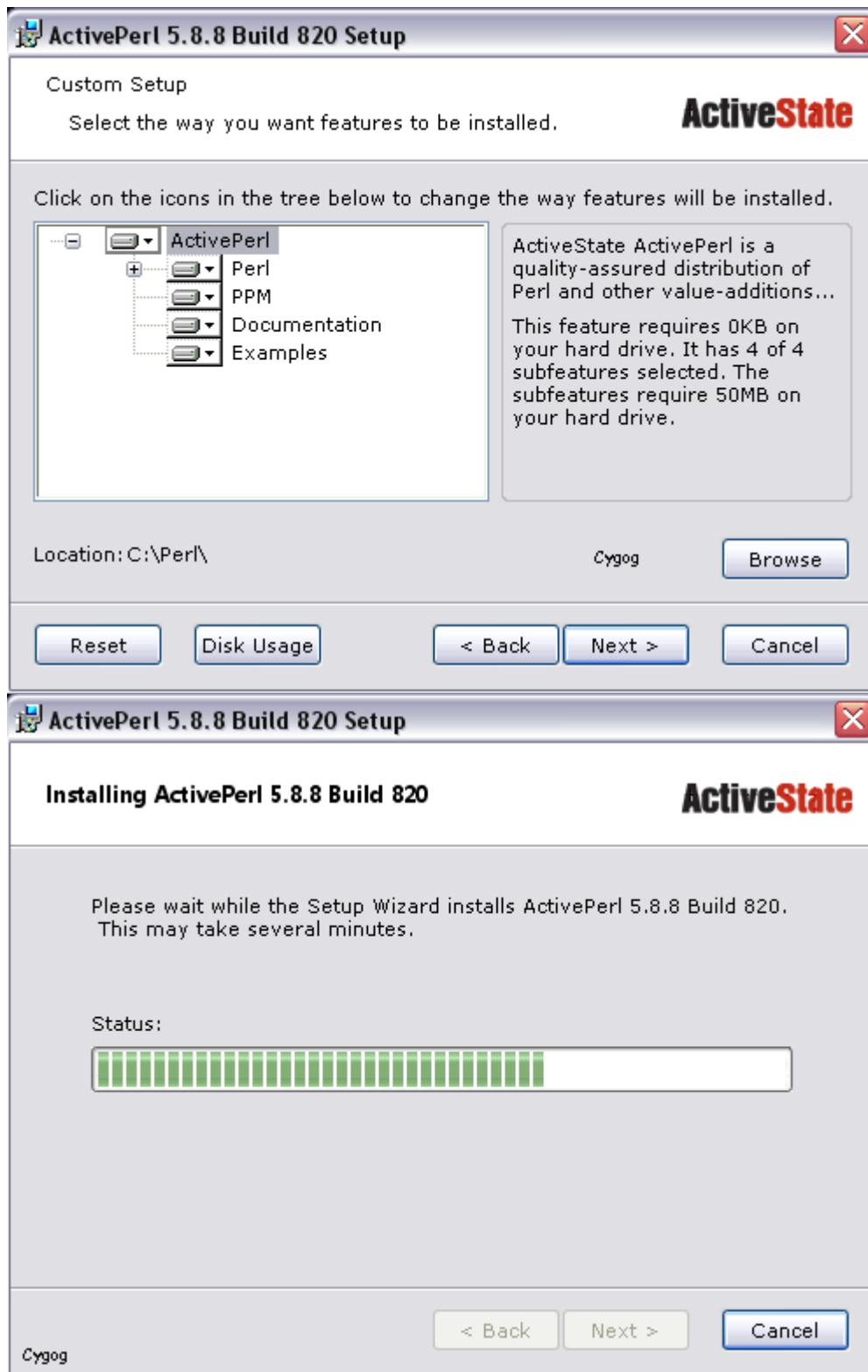
## Compilando códigos Perl.

Ya conociendo la vulnerabilidad a explotar y teniendo el exploit para llevarlo a cabo, faltaría solo compilarlo o interpretarlo para poder atacar al código vulnerable.

1-Descargamos e instalamos el Active Perl Que se puede descargar desde el siguiente link de forma gratuita: <http://downloads.activestate.com>

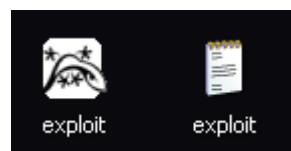
Esto hará que la PC sepa como interpretar los códigos en el sistema.



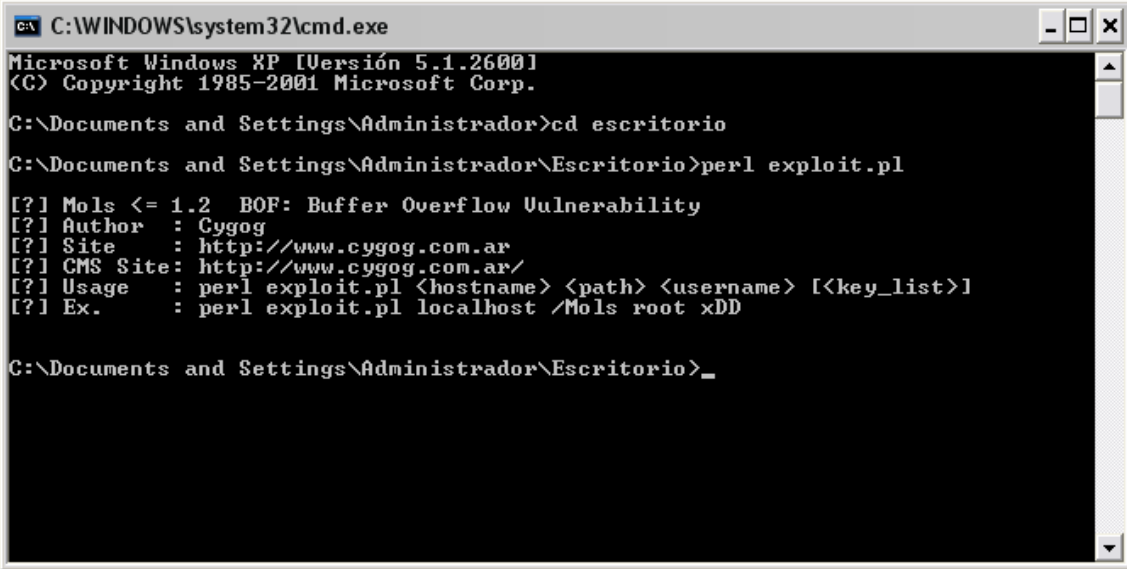


2-Ya instalado, tenemos que generar el código para que sea compilado: *Bloc de notas => Pegamos el exploit => Guardar como.. (en el escritorio) => exploit.pl*

Una vez hecho esto se generará otro archivo con un ícono diferente (quizás un cuadrado con un círculo, o un sombrero negro).. El ícono que lo recuadre en rojo es el exploit guardado con la extensión .pl



3- Ahora ejecutamos el exploit desde MS-DOS para que sea compilado o interpretado: *Inicio => ejecutar => cmd => cd escritorio => perl exploit.pl*



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>cd escritorio
C:\Documents and Settings\Administrador\Escritorio>perl exploit.pl

[?] Mols <= 1.2  BOF: Buffer Overflow Vulnerability
[?] Author   : Cygog
[?] Site     : http://www.cygog.com.ar
[?] CMS Site : http://www.cygog.com.ar/
[?] Usage   : perl exploit.pl <hostname> <path> <username> [<key_list>]
[?] Ex.     : perl exploit.pl localhost /Mols root xDD

C:\Documents and Settings\Administrador\Escritorio>_
```

Bueno como ven aparecen opciones en el exploit para ejecutarlo remotamente.. por ejemplo el mio para ejecutarlo contra una web se debe ejecutar asi: *perl exploit.pl [www.cygog.com](http://www.cygog.com) <algo> <Cygog>*

Listo ya hasta aquí termina esto, ahora les enseñare otra forma para que quede mas claro como compilar en perl. Esta vez usaremos otro software el Perl Express que lo pueden descargar desde aquí: <http://www.perl-express.com/download.html>

### Que es Perl Express? (Según su web)

Perl Express es una única y potente entorno de desarrollo integrado (IDE) bajo Windows 98/ME/2000/XP/2003, incluye varias herramientas para escribir y depurar sus programas perl.

Perl Express está destinado tanto para los profesionales experimentados y desarrolladores de Perl y para los principiantes.

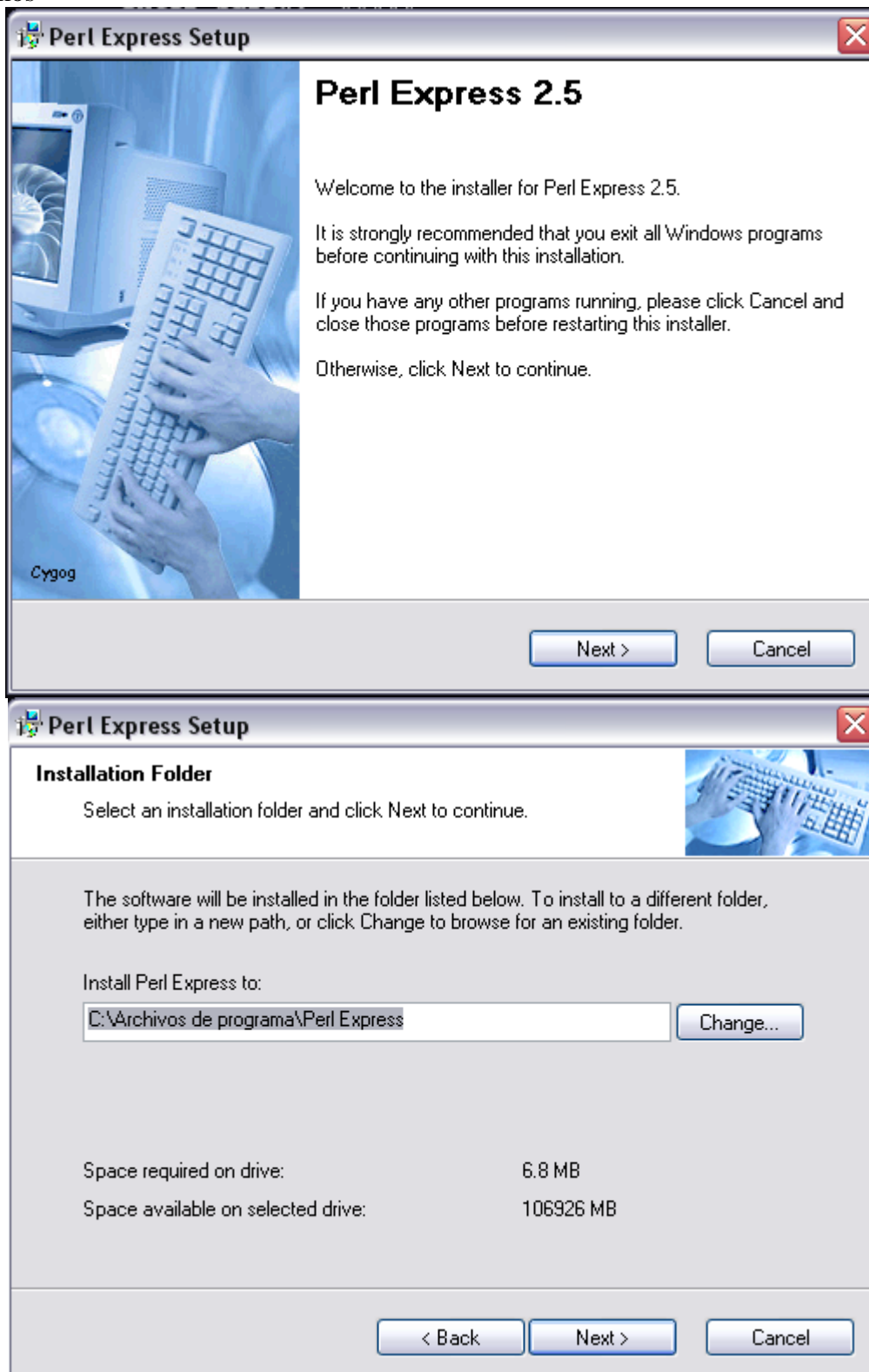
Desde la versión 2.5, Perl Express es software libre, sin limitación, el registro no es necesario.

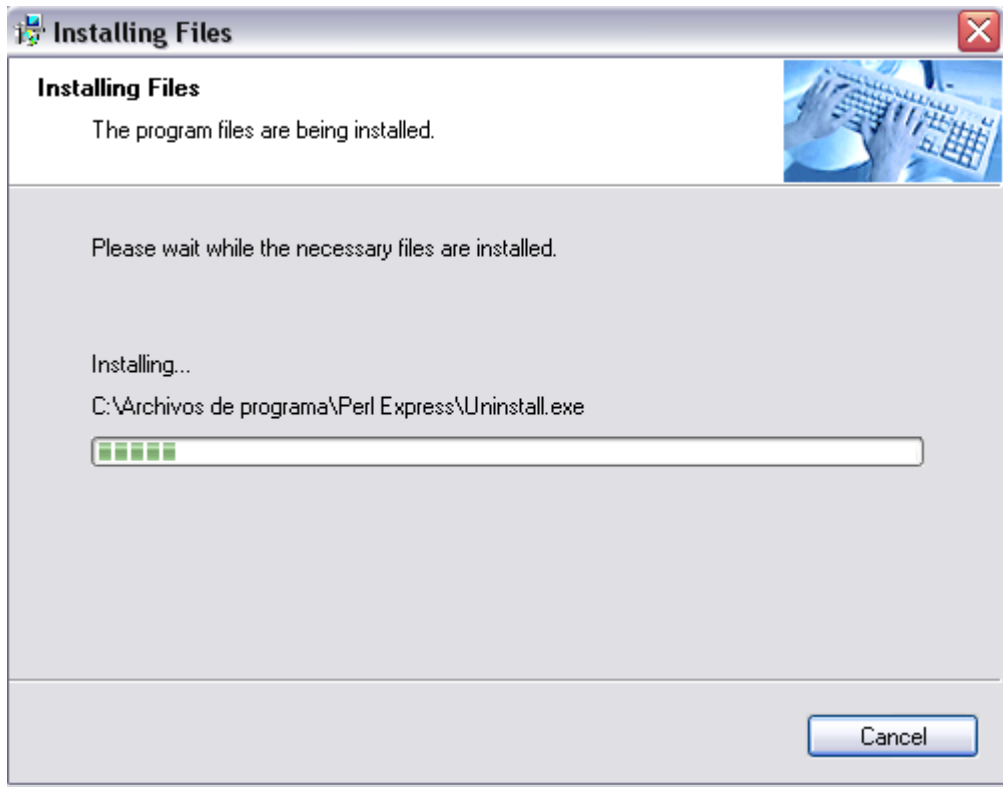
### Características Generales

- Múltiples para la edición de secuencias de comandos, ejecutar y depurar
- Completo servidor de simulación
- Completamente integrado con la depuración de interrupción, el refuerzo, mostrando los valores de las variables, etc
- Las consultas pueden ser creados a partir de navegador Web interno o de consulta de editor
- Prueba de MySQL, MS Access ... guiones para Windows
- interactiva de E / S
- Múltiples archivos de entrada
- Permite configurar las variables de entorno utilizado para ejecutar y depurar script
- Personalizable editor de código con resaltado de sintaxis, el tamaño del texto ilimitado, la impresión, la numeración de línea, marcadores, en la columna de selección, potente motor de búsqueda y reemplazo, múltiples deshacer / rehacer las operaciones de margen y el canal, etc
- Resaltar llaves de la misma
- Windows / Unix / Mac línea terminaciones apoyo
- OfficeXP estilo menú y barras de herramientas
- HTML, RTF exportación
- Vive una vista previa de los scripts en el navegador Web interno
- Directorio de la ventana
- Código de la Biblioteca
- La operación con los proyectos

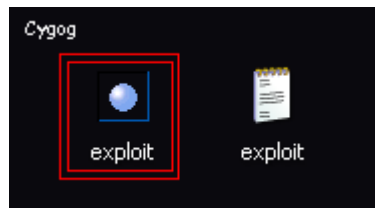
- Ayuda sobre las funciones
- Perl impresora, visor pod, tabla de caracteres y símbolos de HTML, y otros

1- Lo instalamos

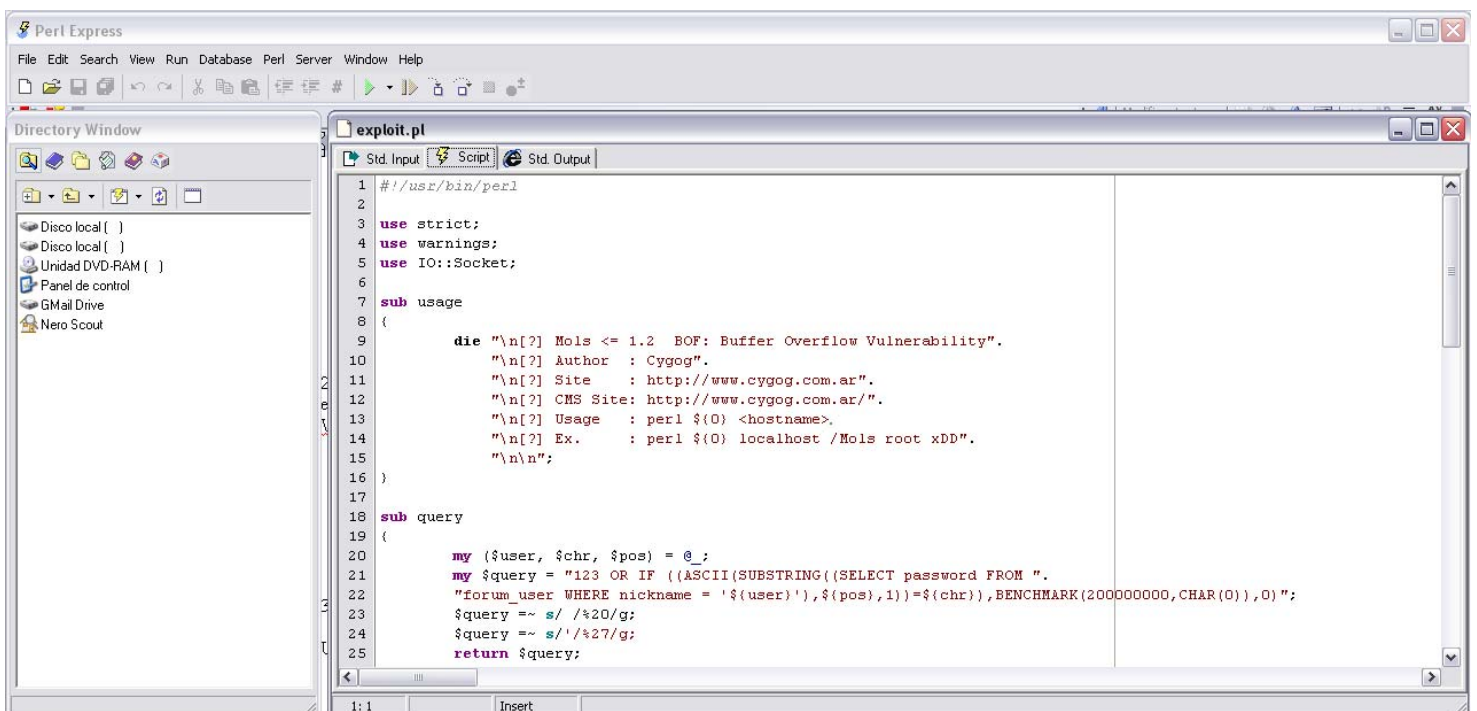




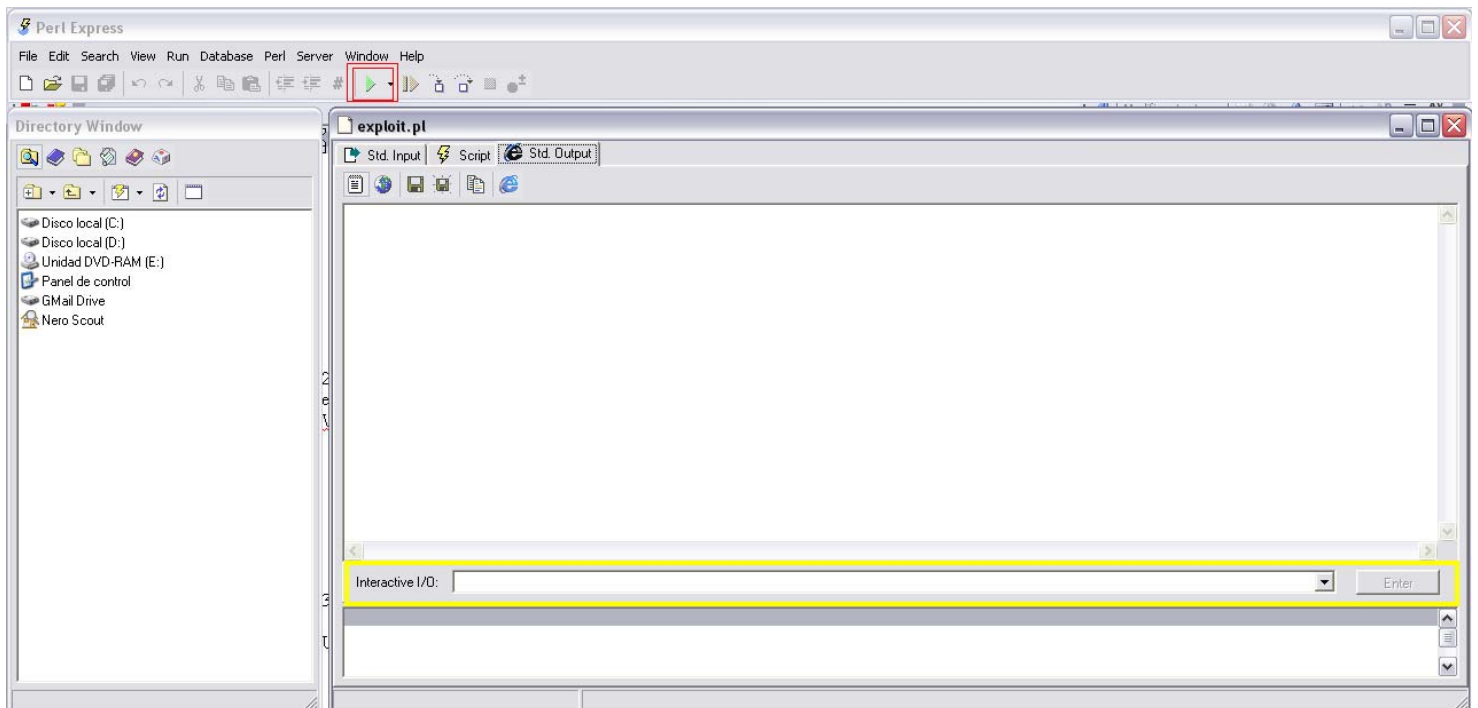
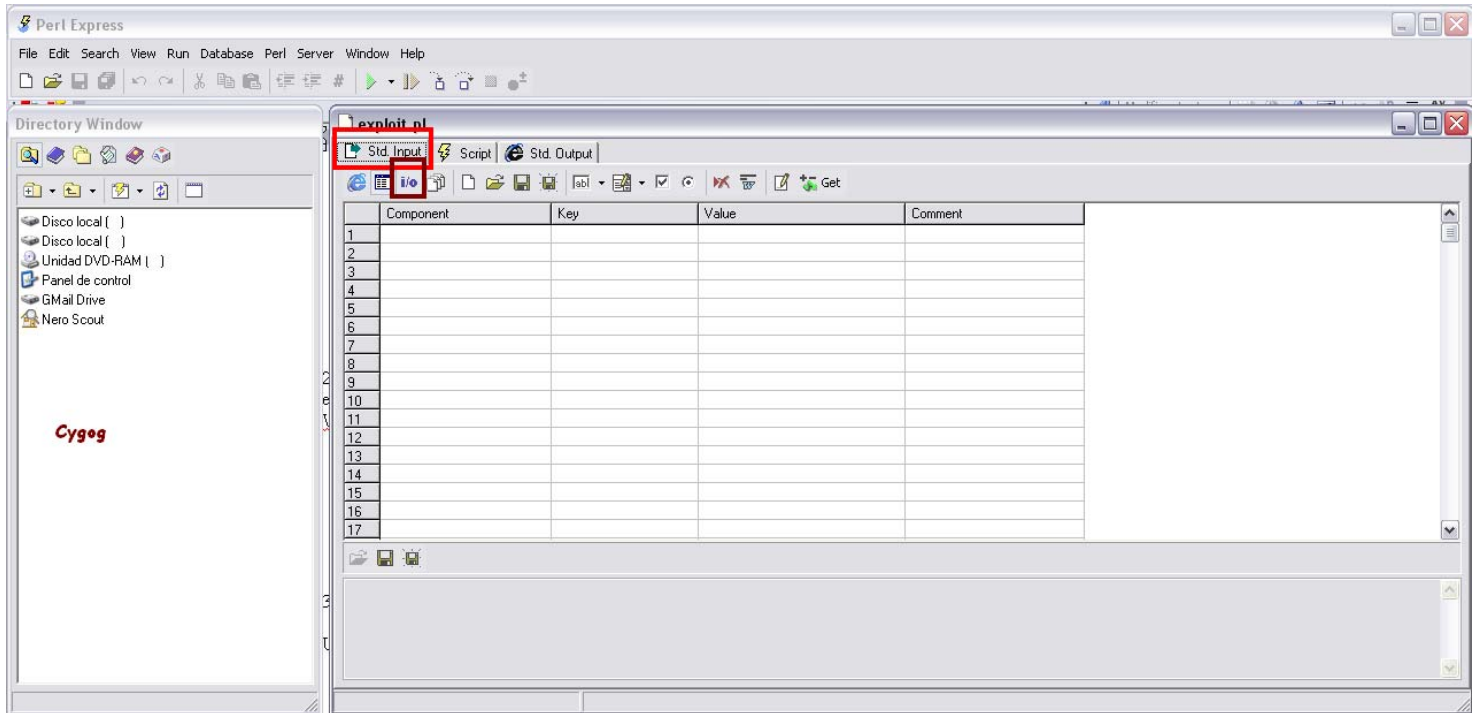
2-Una vez instalado, recuerden que en el otro método de compilación guardábamos el exploit con la extensión “.pl” esta vez hacemos lo mismo y la guardamos en algún directorio que elijan.. En mi caso otra vez en el escritorio. Veran que esta vez se genera otro icono, ya que este software asocia las extensiones .pl (lo recuadré en rojo)



3-Abrimos el software Perl Express, y clickeamos: file => open => exploit.pl (el mío estaba en el escritorio) Una vez esto abrirá el exploit.



Vamos a la carilla resaltada en rojo y le damos clic en I/o (interactivo) para que se interprete y podremos como bien dice la palabra interactuar con el exploit.



Luego le damos en la flecha verde (que resalte en rojo) y ya se abra ejecutado en exploit.. Ahora solo debemos ejecutarla remotamente.. Para esto usamos la barra de interactividad. Solo tenemos que poner lo que el exploit nos demande, por ejemplo [www.cygog.com](http://www.cygog.com) `-i imgs -d` Luego le damos clic en enter y el exploit estará ejecutándose.

Bueno espero que estas dos maneras les haya quedado claro.

## Compilando códigos c y c++

Anteriormente les dije como se los identificaba, una vez teniendo la vulnerabilidad y el exploit para explotarla, tendremos que compilarlo y ejecutarlo. Esta vez usaremos un compilador llamado Cygwin.

**¿Que es Cygwin?** Según su web

# Cygwin es tanto para entorno de Linux como para Windows. Consta de dos partes: Una DLL (cygwin1.dll), que actúa como una capa de emulación API de Linux proporciona una API de Linux funcionalidad.

# Una colección de herramientas que ofrecen Linux y sentir.

La DLL de Cygwin actualmente trabaja con todos los últimos, comercialmente en x86 de 32 bits y 64 bits versiones de Windows, con la excepción de Windows CE.

Tenga en cuenta que el apoyo oficial para Windows 95, Windows 98 y Windows Me se suspenderá con la próxima versión (1.7.0) de Cygwin.

**¿Qué es Cygwin no?**

# Cygwin no es una forma de ejecutar aplicaciones nativas de Linux en Windows. Tienes que reconstruir su aplicación desde el código fuente si desea que se ejecute en Windows.

# Cygwin no es una manera de hacer arte de magia aplicaciones nativas de Windows UNIX® consciente de funcionalidad, como señales, ptys, etc Una vez más, usted necesita para construir sus aplicaciones desde el código fuente si desea aprovechar las ventajas de la funcionalidad de Cygwin.

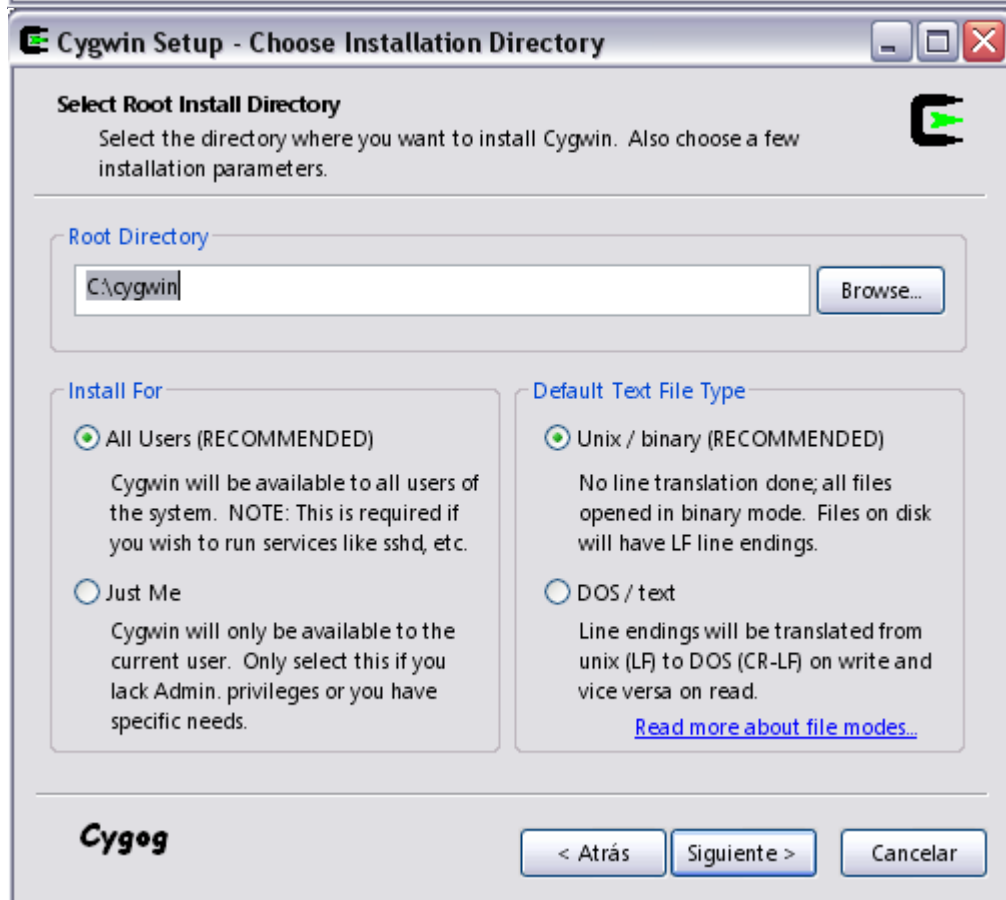
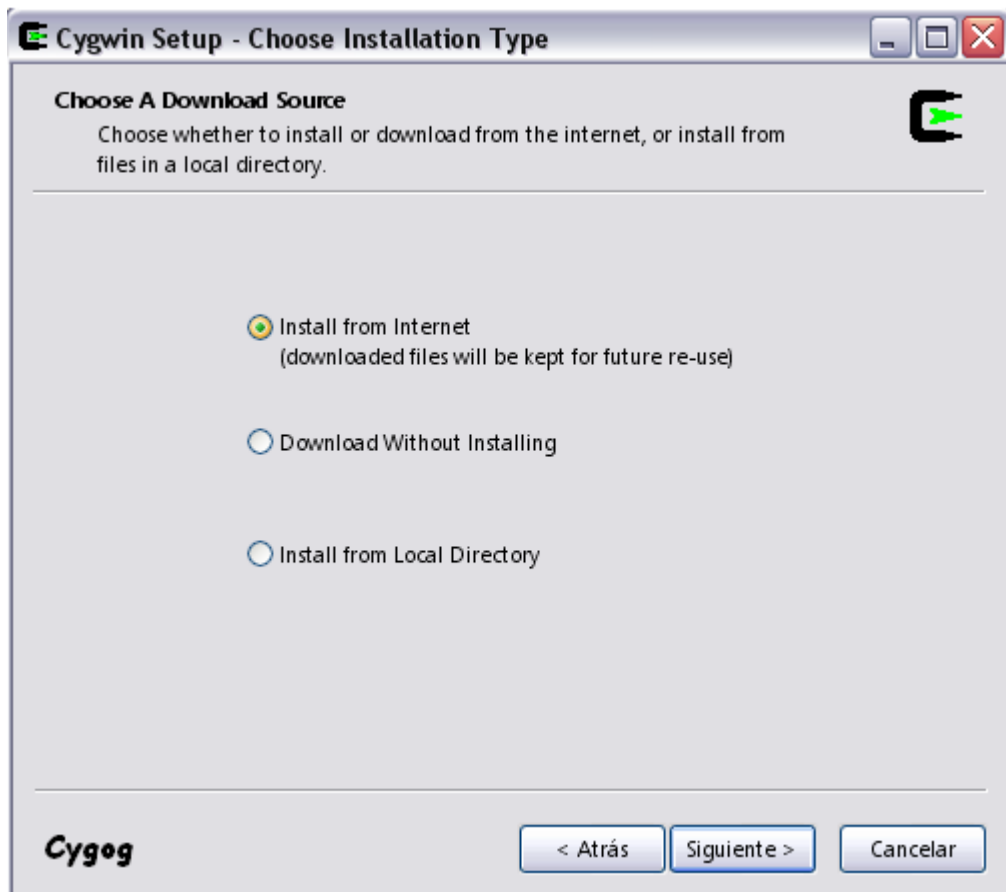
Bueno a continuación dejare un link para que puedan descargarlo:

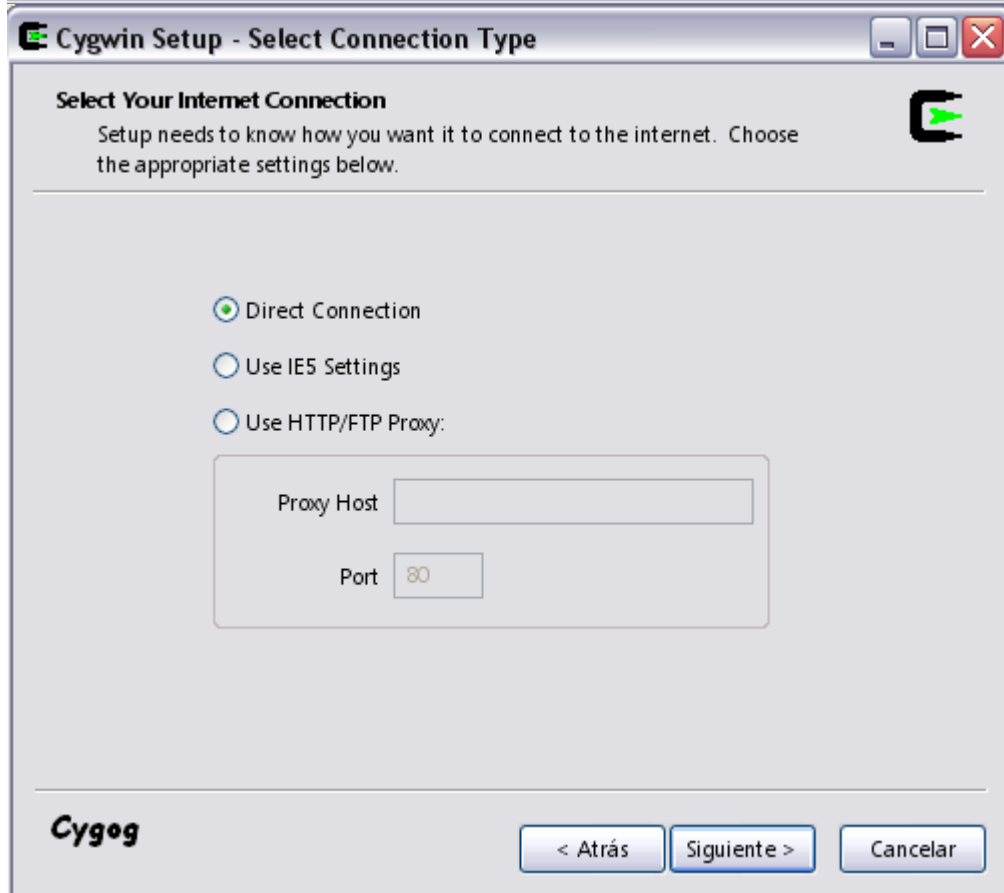
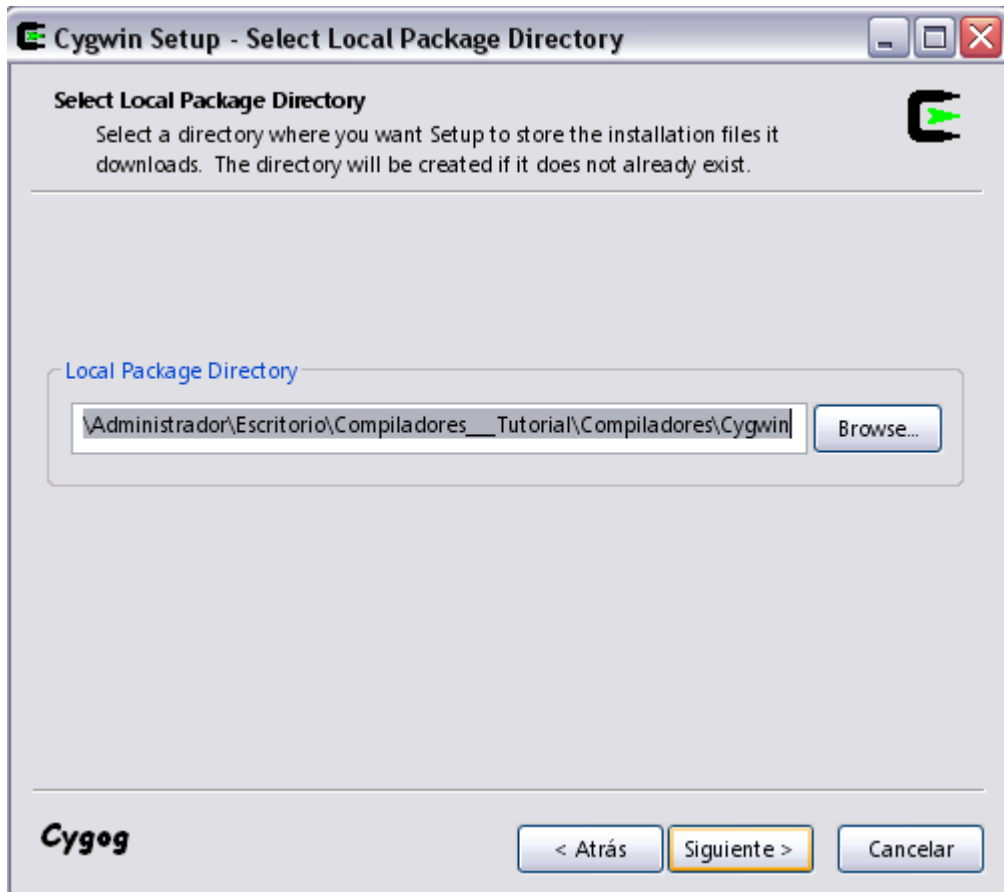
<http://www.cygwin.com/setup.exe>

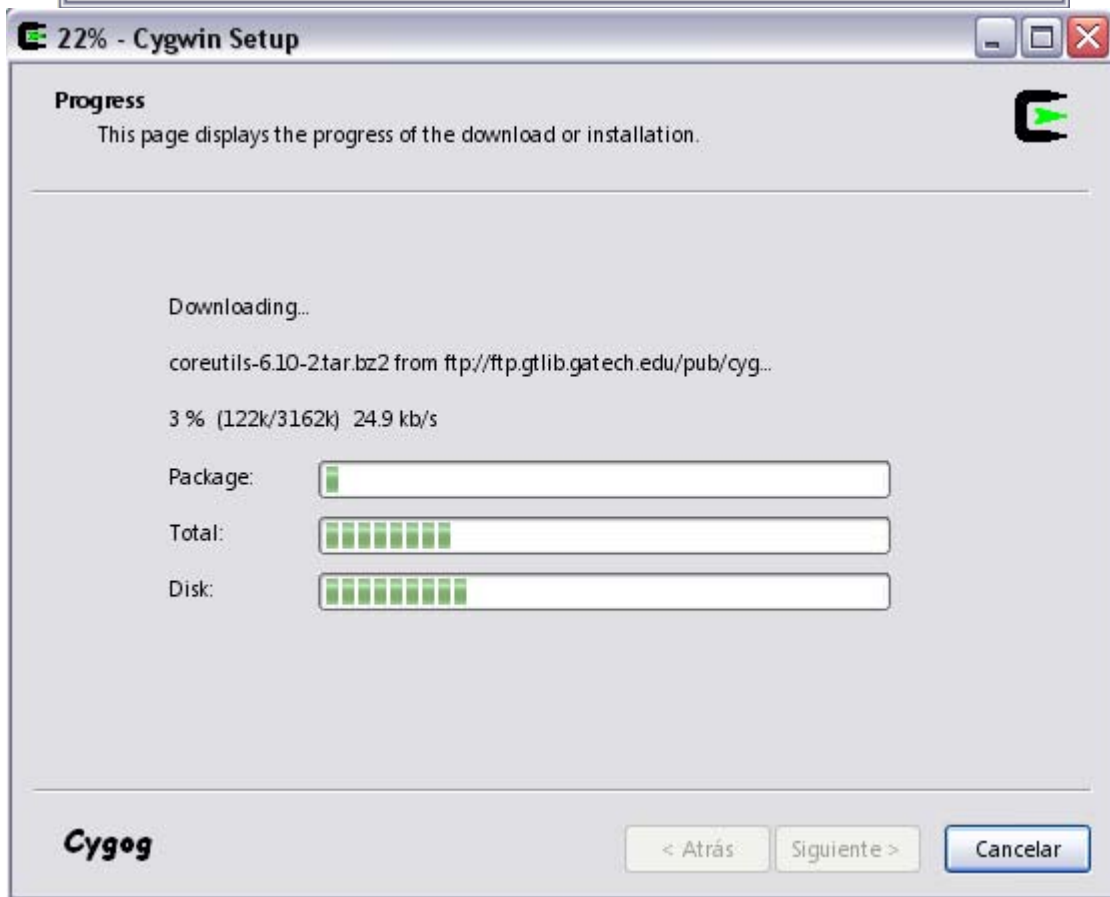
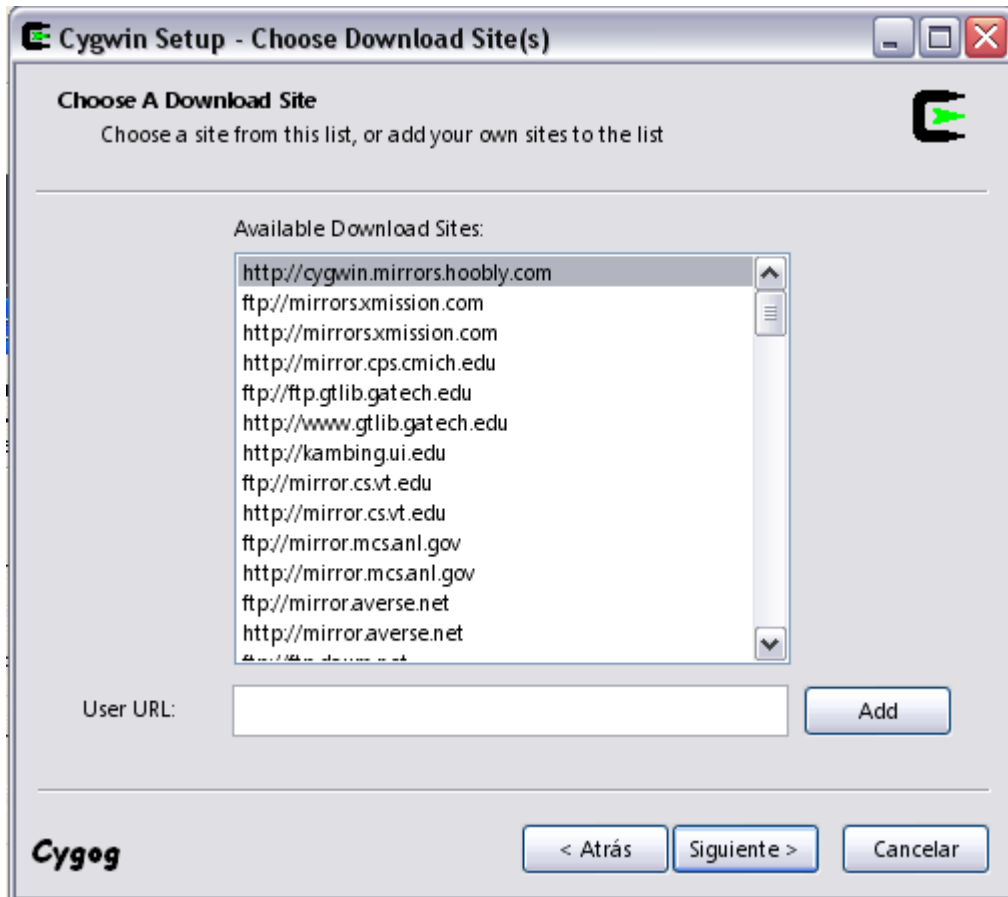
Unas ves descargado, instalamos:

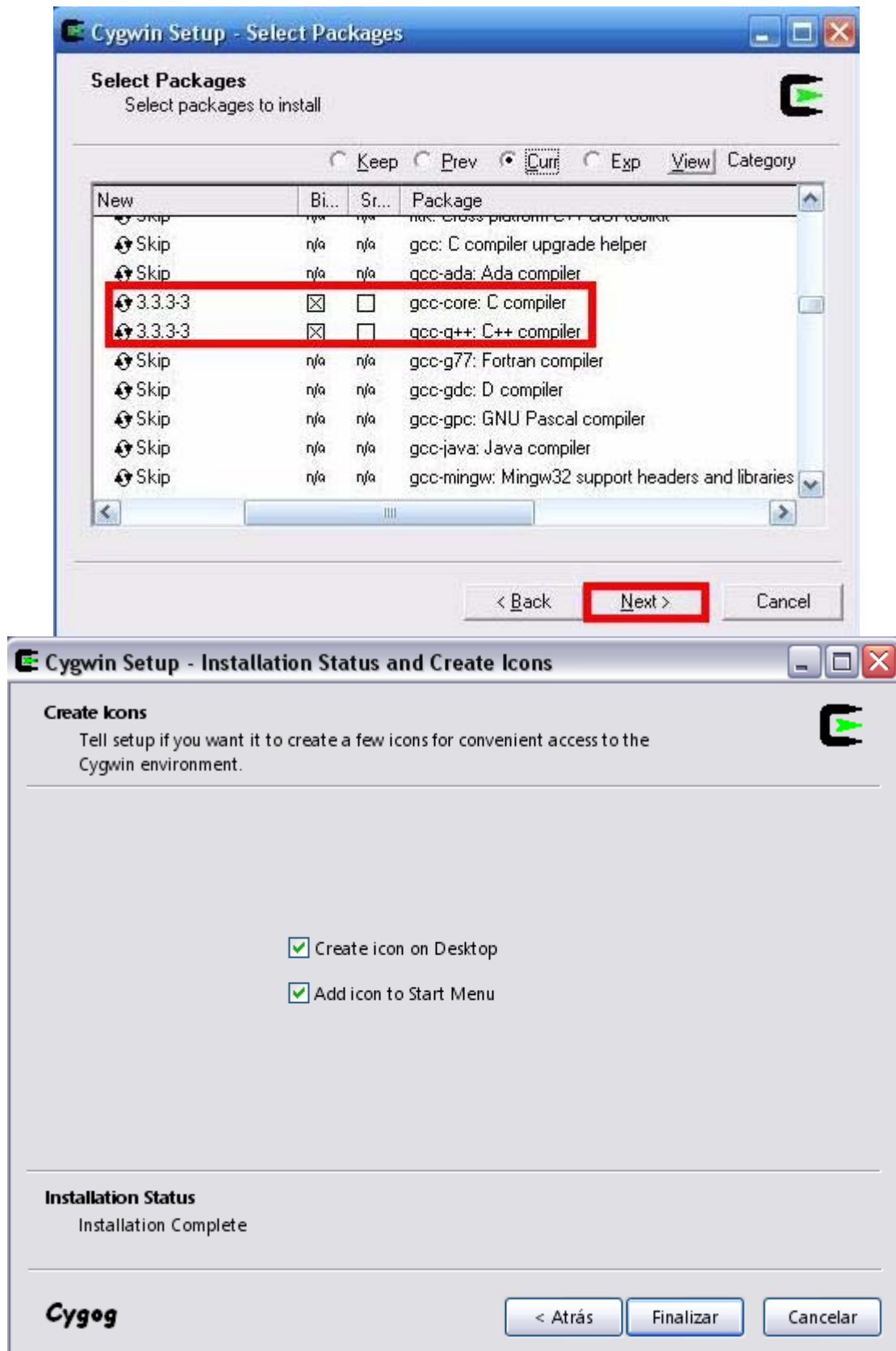




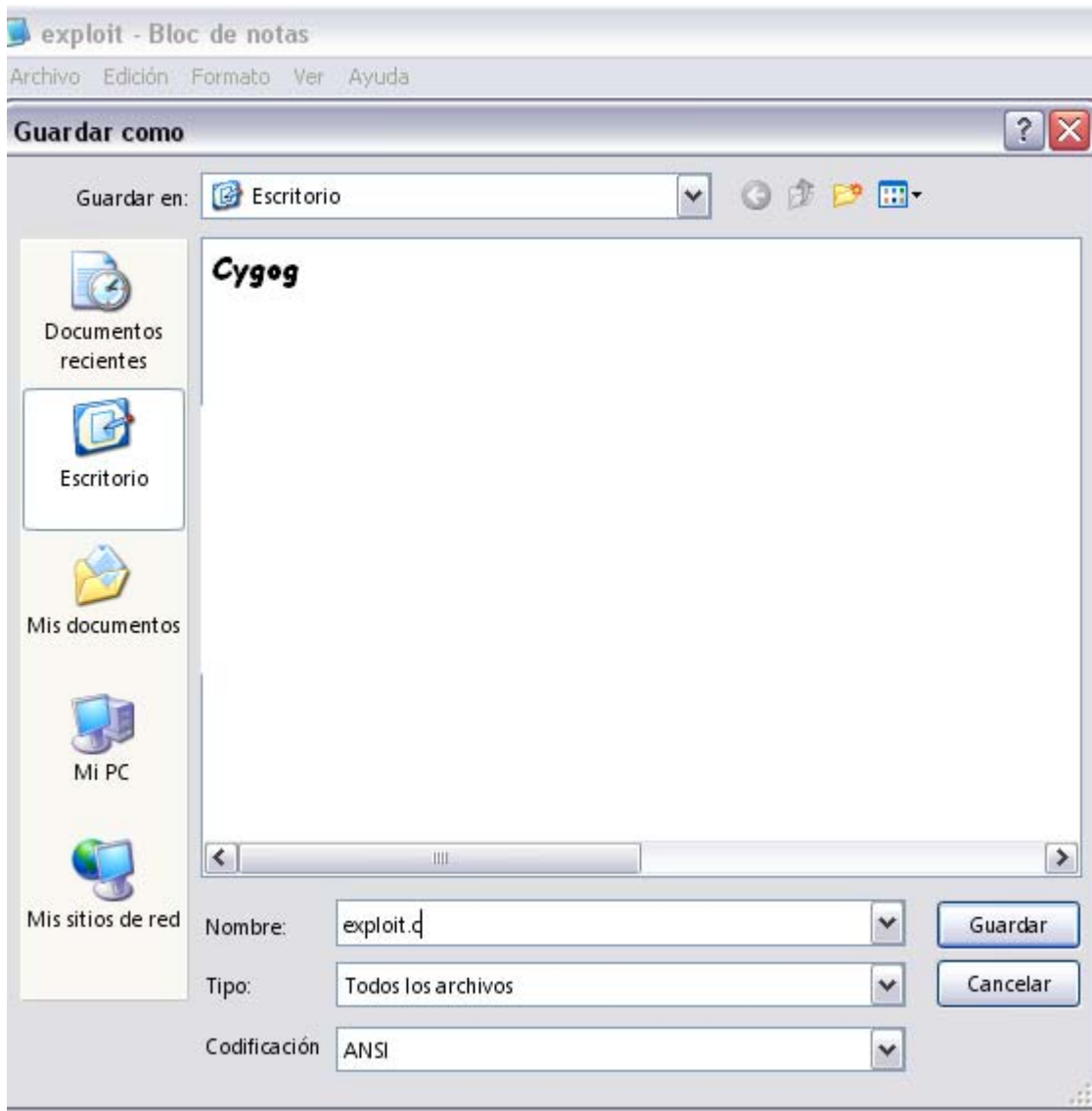








Una vez que este instalado, solo faltaría guardar el exploit con el bloc de notas con la extensión ".c" *guardar como.. exploit.c*



Lo guardamos en la carpeta `c:\cygwin\bin`. Ahora lo compilamos a exe:  
Inicio – ejecutar – cmd – (nos situamos en la carpeta bin)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrador>CD..
C:\Documents and Settings>CD..
C:\>CD CYGWIN
C:\cygwin>CD BIN
C:\cygwin\bin>
```

*CYGOG* El mal de parkingson

Ejecutamos el comando `gcc exploit.c -o exploit.exe` para que nuestro exploit se compile a .exe



```
C:\WINDOWS\system32\cmd.exe
C:\cygwin\bin>gcc exploit.c -o exploit.exe
C:\cygwin\bin>
```

Cygog

Si volvimos a la carpeta bin otra vez es porque el exploit se compilo correctamente! Ahora lo ejecutamos desde el ms- dos otra vez:



```
C:\WINDOWS\system32\cmd.exe
C:\cygwin\bin>gcc exploit.c -o exploit.exe
C:\cygwin\bin>exploit.exe
Stack pointer (ESP) : 0x22cc78
Offset from ESP : 0x0
Desired Return Addr : 0x22cc78
C:\cygwin\bin>_
```

Cygog

Bueno espero que hayan entendido, ya hemos terminado, este exploit ya lo hemos ejecutado.. Cualquier duda consultar en el email [Cygog@live.com.ar](mailto:Cygog@live.com.ar)

## Interpretación y compilación de códigos PHP

Php es un código que es interpretado, pero cuando se convierte en .exe se es compilado. La herramienta que usaremos es el BamCompile, que lo pueden descargar desde este

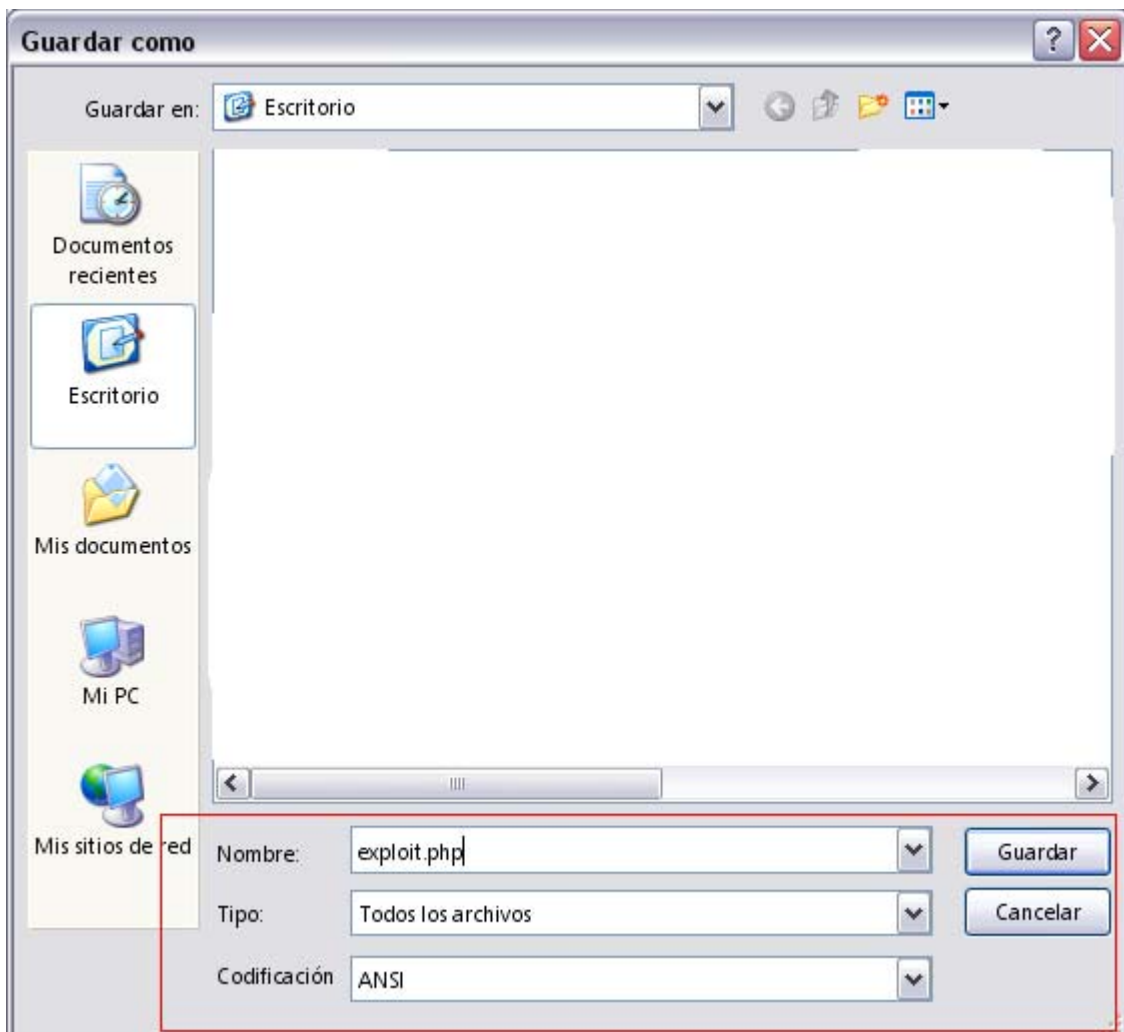
<http://www.bambalam.se/bamcompile/download/bamcompile1.21.zip>

- ¿Qué es? (Defenicion sacada desde su web)

Bambalam PHP EXE Compiler/Embedder is a free command line tool to convert PHP applications to standalone Windows .exe applications. Compilador PHP Bambalam EXE / Embedder es un servicio gratuito de línea de comando herramienta para convertir aplicaciones PHP para Windows independiente. Exe aplicaciones. The exe files produced are totally standalone, no need for php dlls etc. The php code is encoded using the [Turck MMCache Encode library](#) so it's a perfect solution if you want to distribute your application while protecting your source code. El exe producidos son totalmente independiente, sin necesidad de php dlls etc El código PHP está codificada utilizando el [Turck MMCache Codifican biblioteca](#) por lo que es una solución perfecta si quieres distribuir tu aplicación, mientras que la protección de su código fuente. The converter is also suitable for producing .exe files for windowed PHP applications (created using for example the [WinBinder library](#) ). It's also good for making stand-alone PHP Socket servers/clients (using the php\_sockets.dll extension). El convertidor también es adecuado para la producción. Exe ventanas para aplicaciones PHP (por ejemplo, creado con la [WinBinder biblioteca](#)). También es bueno para hacer stand-alone PHP Socket servidores / clientes (utilizando la extensión php\_sockets.dll).

Una ves ya lo tengas en su pc lo descomprimimos y lo ubicamos en el escritorio.

Teniendo un exploit en php nos queda guardarlo con una extencion .php



Ahora compilamos el exploit que tiene una extensión .php a .exe.  
Abrimos el cmd y ejecutamos de la siguiente manera:

*CD ESCRITORIO**CD bamcompile**Bamcompile exploit.php exploit.exe*

```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrador>CD ESCRITORIO
C:\Documents and Settings\Administrador\Escritorio>CD BAMCOMPILE
El sistema no puede hallar la ruta especificada.
C:\Documents and Settings\Administrador\Escritorio>CD BAMCOMPILE

C:\Documents and Settings\Administrador\Escritorio\bamcompile>bamcompile exploit
.php exploit.exe

Bambalam PHP EXE Compiler/Embedder 1.21
Mainfile: exploit.php
Outfile: exploit.exe

Encoding and embedding exploit.php
exploit.exe created successfully!
C:\Documents and Settings\Administrador\Escritorio\bamcompile>
```

Listo! Ya tenemos el exploit en exe ahora solo nos queda ejecutarlo:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrador>CD ESCRITORIO
C:\Documents and Settings\Administrador\Escritorio>CD BAMCOMPILE
C:\Documents and Settings\Administrador\Escritorio\bamcompile>exploit.exe
#!/usr/bin/php -q

phpslash <= 0.8.1.1 Remote Code Execution Exploit
-----
About:
by DarkFig < gmdarkfig (at) gmail (dot) com >
http://acid-root.new.fr/
#acidroot@irc.worldnet.net

Usage:
php spl.php -url <website> [options]

Example:
php spl.php -url http://victim.com/

Options:
-proxhost <ip:port> if you wanna use a proxy
-proxauth <usr:pwd> proxy with authentication
C:\Documents and Settings\Administrador\Escritorio\bamcompile>
```

Listo ahora solo nos quedaría seguir las instrucciones de uso que tiene..



## Compilando códigos Python

Bueno para compilar códigos escritos en Python tendremos que utilizar una herramienta llamada Active Python El cual se puede descargar de forma gratuita desde el siguiente link:

<http://www.python.org/download/>

Ya teniendo un exploit escrito en Python solo nos queda abrir el bloc de notas y guardarlo en el escritorio con la extensión “.py”. Nos aparecerá algo haci:



Ahora solo nos falta ejecutarlo:

*Abrimos el cmd*

*CD ESCRITORIO*

*exploit.py*

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>CD ESCRITORIO
C:\Documents and Settings\Administrador\Escritorio>exploit.py
-----
BlazeVideo HDTV Player <= 3.5 Playlist File Remote Heap Overflow Exploit
by LiquidWorm [liquidworm[at]gmail.com] - 2009
-----
Traceback (most recent call last):
  File "C:\Documents and Settings\Administrador\Escritorio\exploit.py", line 72,
in <module>
    payload = garbage + eip + nop + shellcode + nop
NameError: name 'garbage' is not defined

C:\Documents and Settings\Administrador\Escritorio>_
```

Cygog

Bueno ya hemos ejecutado este exploit! Jejeje solo faltaria seguir sus instrucciones para hacerlo “explotar” contra una vulnerabilidad! (en este caso es un exploit para BlazeVideo 3.5 xD)

Bueno, esto es todo, espero que les haya gustado y hasta la próxima.

Atte. Cygog (Cygog@live.com.ar)