[How to Use PowerShell Empire Getting Started with Post-Exploitation of Windows Hosts](https://null-byte.wonderhowto.com/how-to/use-powershell-empire-getting-started-with-post-exploitation-windows-hosts-0178664/)

[PowerShell Empire](https://www.powershellempire.com) is a post-exploitation framework for computers and servers running Microsoft Windows, Windows Server operating systems, or both. In these tutorials, we will be exploring everything from how to install Powershell Empire to how to snoop around a victim's computer without the antivirus software knowing about it. If we are lucky, we might even be able to obtain domain administrator credentials and own the whole network.

**A Tool for Targeting Windows**

Exploit frameworks are popular, and most hackers have heard of [Metasploit](../../../../docs/Technology/Hacking/ExploitDatabase/%20Metasploit.pdf), a framework that automates the deployment of powerful exploits. You may be asking yourself, how does PowerShell Empire differ from Metasploit? Isn't Metasploit already serving the same purpose? Well, yes and no. PowerShell Empire deals strictly with Windows machines, and it is extremely useful in a penetration test because most targets these days are running some version of Windows.

**Don't Miss:** [**The Ultimate Command Sheet for Metasploit's Meterpreter**](../../../../docs/Technology/Hacking/ExploitDatabase/%20Metasploit.pdf)

A simple example of this point would be the widespread usage of excel on Microsoft Windows. Since Microsoft Excel has more advanced features than the Mac version (as well as Office 365), we can assume that the finance department of most target companies will be using Microsoft Windows. Finance departments also usually have access to bank account numbers and other juicy data!

PowerShell Empire also gives the attacker the ability to run commands in memory. This means that the malicious actions being taken by PowerShell Empire are not run on the hard drive, they are instead run in the computer's memory. This reduces the likelihood of being caught by antivirus software as well as the likelihood of leaving digital fingerprints for forensics investigators.

When to Use PowerShell Empire

Some of the activities and goals that can be accomplished include privilege escalation (elevating privileges from a standard user account to an administrator), network and host reconnaissance (finding out what hosts and services are present), lateral movement between hosts, and the gathering of credentials. All of these are key components of a modern day penetration test.

PowerShell Empire accomplishes this via three main components: listeners, stagers, and agents.

* A listener is a process which listens for a connection from the machine we are attacking. This helps Empire send the loot back to the attacker's computer.
* A stager is a snippet of code that allows our malicious code to be run via the agent on the compromised host.
* An agent is a program that maintains a connection between your computer and the compromised host.

Lastly, modules are where the fun is. These are what execute our malicious commands, which can harvest credentials and escalate our privileges as mentioned above.

Now that we have discussed what PowerShell Empire does and why it is useful, let's take a look at how to get it up and running.

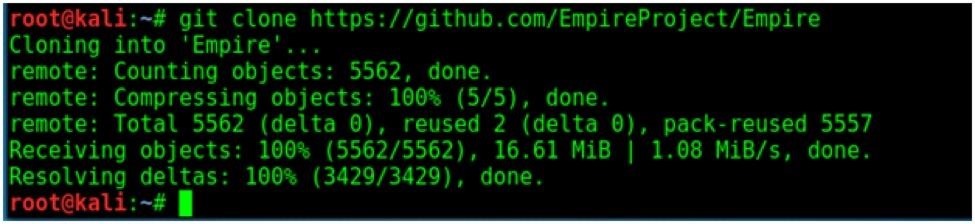
Step 1 Installing PowerShell Empire

To run Powershell, you will need a Kali Linux machine. If you need a good starter Kali computer for hacking, you can check out our guide on setting one up on the [low-cost Raspberry Pi](https://www.amazon.de/CanaKit-Raspberry-Complete-Starter-Kit/dp/B01C6Q2GSY/?tag=wnbde-21&language=en_GB) below.

**Learn More:** [**Build a Kali Linux Hacking Computer on the Raspberry Pi**](https://null-byte.wonderhowto.com/how-to/set-up-headless-raspberry-pi-hacking-platform-running-kali-linux-0176182/)

To install Empire on your Kali Linux machine, we need to clone it from GitHub. Open a terminal and type the following command as shown below.

git clone <https://github.com/EmpireProject/Empire.git>

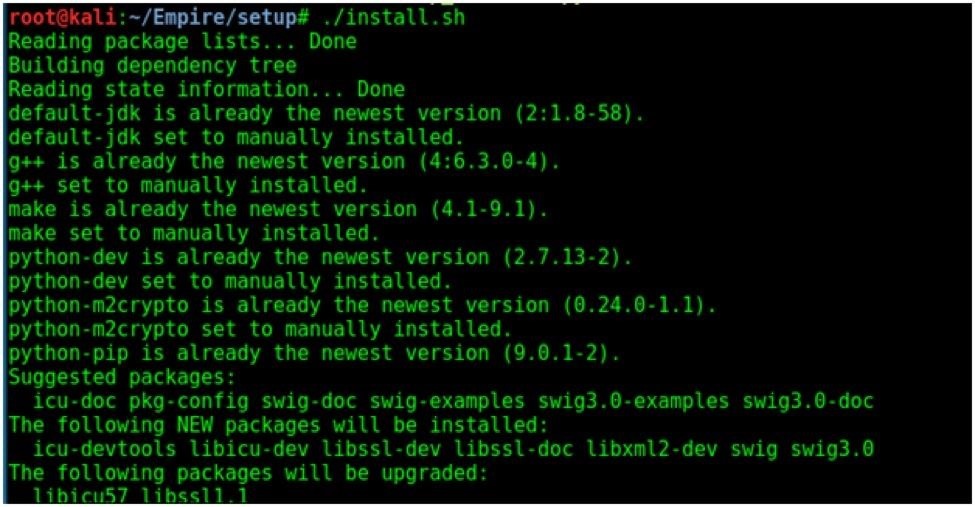


This will create a new directory with the name "Empire." Move into that directory by typing [**cd**](../../../docs/Technology/Hacking/Linux/LinuxUltimateGuide.pdf) **Empire**, then use the [**ls**](../../../docs/Technology/Hacking/Linux/LinuxUltimateGuide.pdf) command to view the contents of the directory.

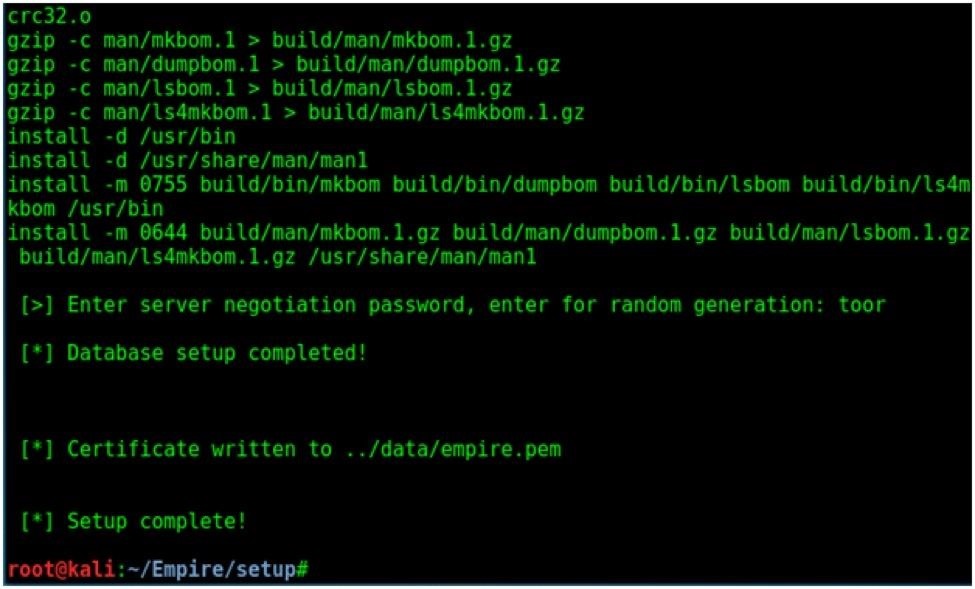
You can read about Empire in the *README.md* file. You will see a "setup" folder inside the Empire directory. Navigate to that folder by typing **cd setup**, then use the **ls** command to view the contents of the "setup" folder. You can see an install shell script as shown below.



Type **./install.sh** to install Empire by running the script. The installation will start as shown below.



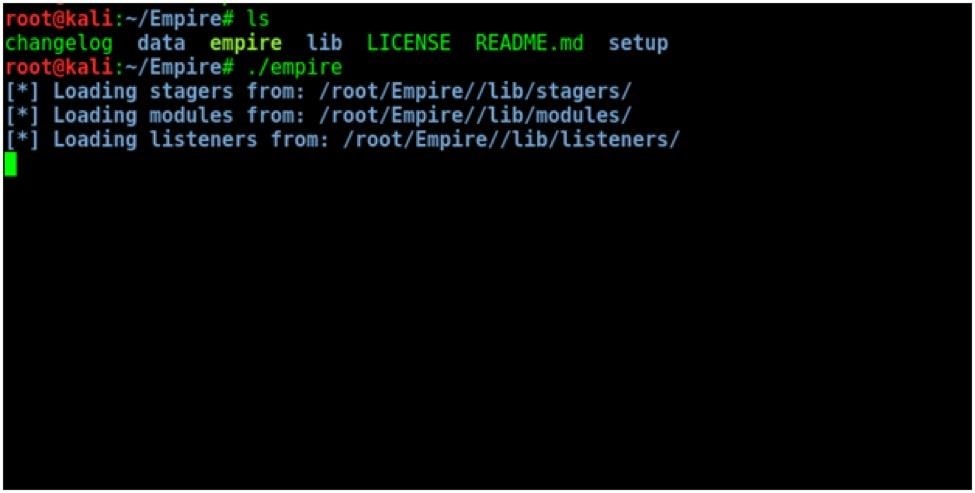
During the installation process, you will be asked to set up a server negotiation password. I set it as "toor,' but you can choose your own password. If everything went well, the installation will finish as shown below.



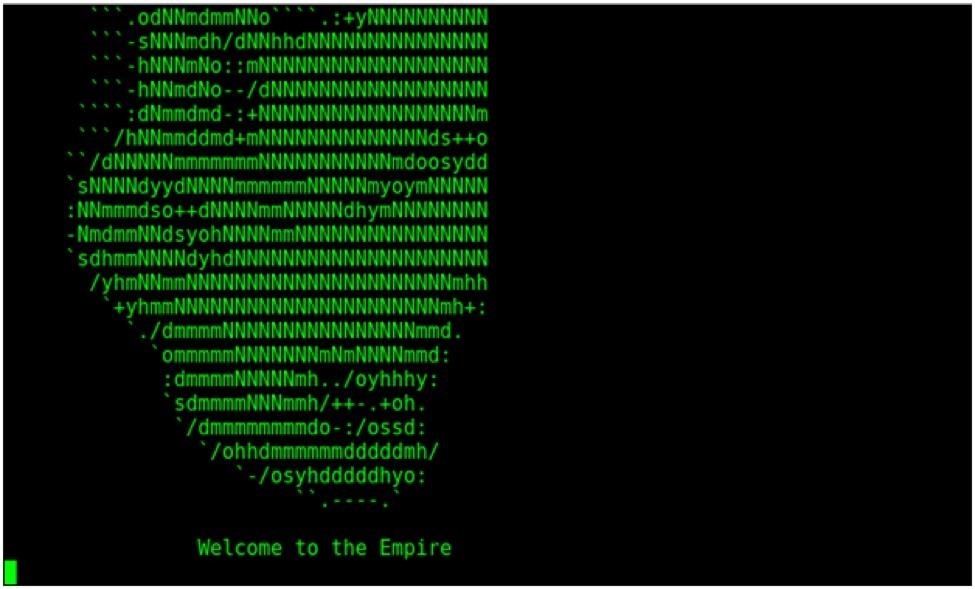
We are done with the installation. Now, it's time to start Empire.

Step 2 Running Powershell Empire

Move back to the Empire directory by typing **cd ..** and run the **./empire** executable as shown. It will start as seen below.



If Empire displays any error while starting, navigate to the "setup" folder with **cd setup** and run the **./reset.sh** script. Then restart Empire again like we did before. It will display a welcome message as shown below.

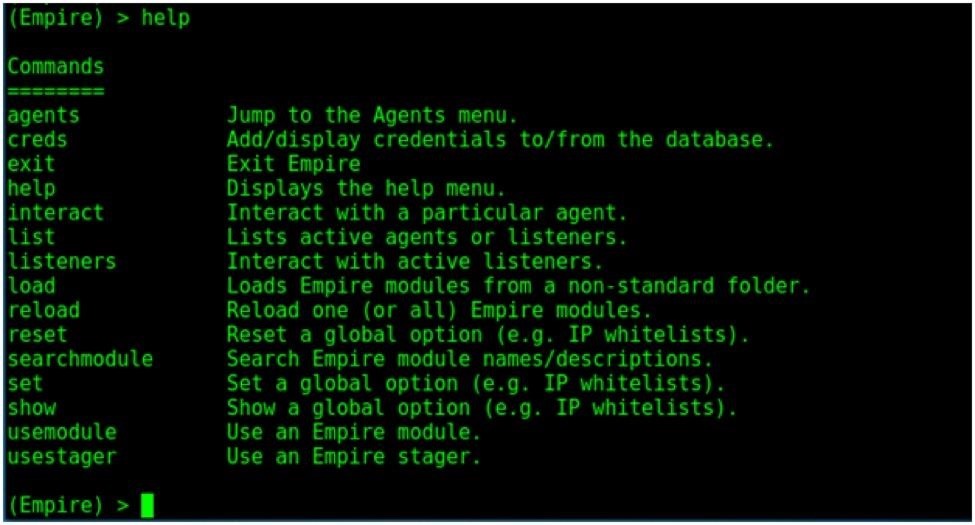


Upon completion, Empire will show the following screen.



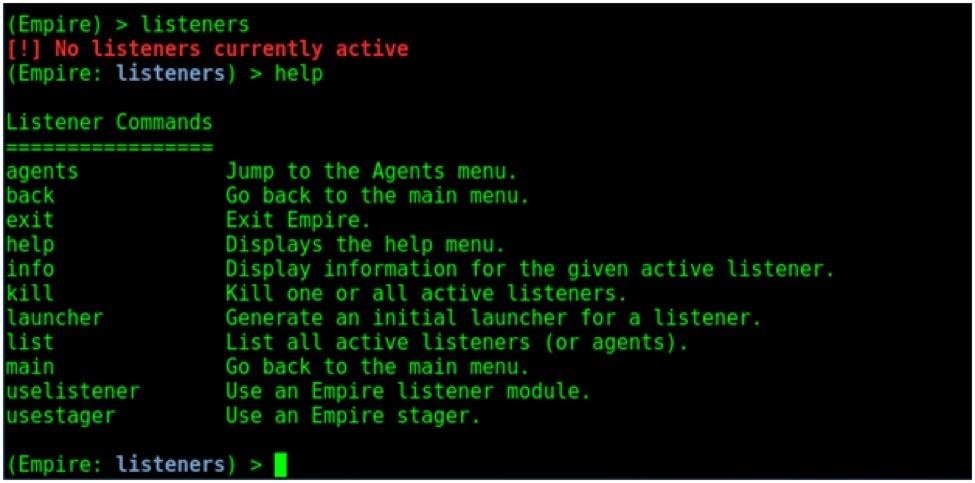
As of this writing, Empire has 267 modules. Don't worry if these sound like complicated ninjitsu techniques; with diligence and practice you will learn what modules, listeners, and agents are. By the end of this series, you will get a clear idea what these are and how to use them.

First, let's start by typing the **help** command. The **help** command will display the help menu as seen below.



Step 3 Using Listeners

[Listeners](https://null-byte.wonderhowto.com/how-to/listeners/) in Empire are the channels which receive connections from our target machine. Before we do anything in Empire, we need to start the listeners. We can move to the listener management menu by typing command **listeners** as shown below.



Once we move to the listeners management menu, as shown above, we can see its sub-menu by typing the **help** command. Let's take a look at what each command will do.

* **agents** - Will allow you to jump to agents menu.
* **back & main** – Will take you back to the main menu.
* **exit** – Will exit from Empire.
* **help** – Will display help menu as shown in the above image.
* **info** – Will display information about the active listener.
* **kill** – Will kill a particular listener.
* **launcher** – Used to generate an initial launcher for a listener.
* **list** – Will list all the active listeners.
* **usestager** – Used to use a stager (we will see below what exactly is a stager).
* **uselistener** – Used to start a listener module.

Let us now look at how to start a listener module in Empire. Type the **uselistener** command, and use tab completion to see the listeners available in Empire.

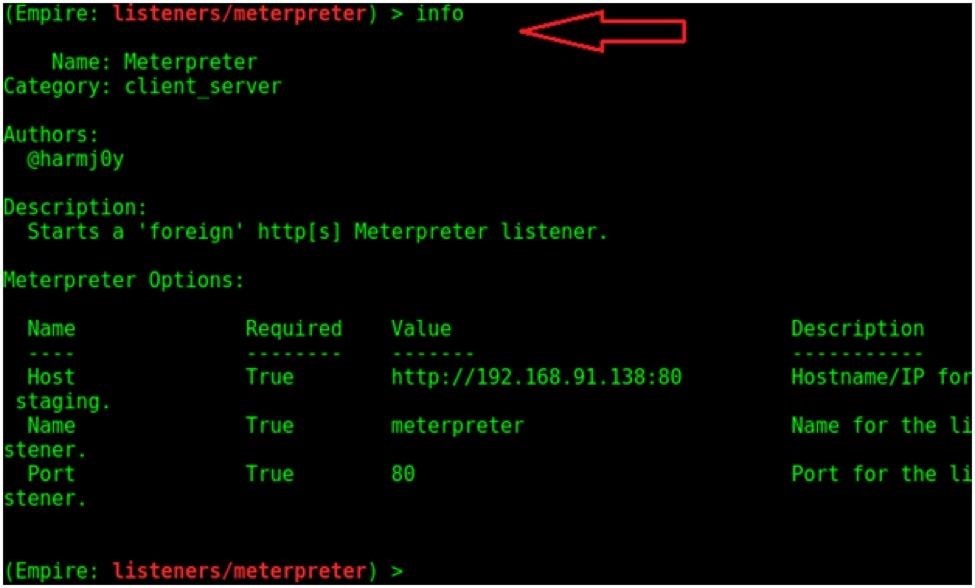


The types of listeners available are shown above. We will learn about different types of listeners in the upcoming sections. For now, let's see how to start a listener.

Let's use the "meterpreter" listener as an example. Type **uselistener meterpreter** as shown above. Once the particular listener is loaded, you can type **help** command to display the available options.

The **agents**, **back**, **exit**, **help**, **launcher**, **listeners**, and **main** commands have been explained above. Let us learn about the other commands.

The **info** command shows the information about the particular type of listener we want to start, as seen below.



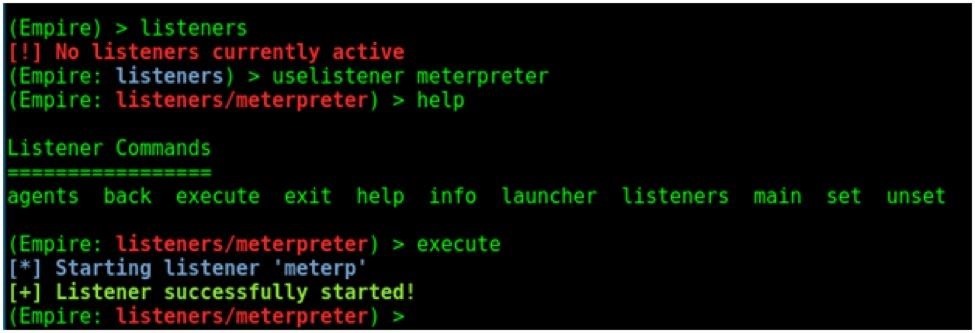
Every listener requires certain options to be set. For example, the "meterpreter" listener needs the *Host* and *Port* values to be configured. The **set** command is used to assign these values. Similarly, the **unset** command is used to clear these values.

**Don't Miss:** [**How to Use Listeners**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-ms-word-embed-listener-your-roommates-computer-0140868/)

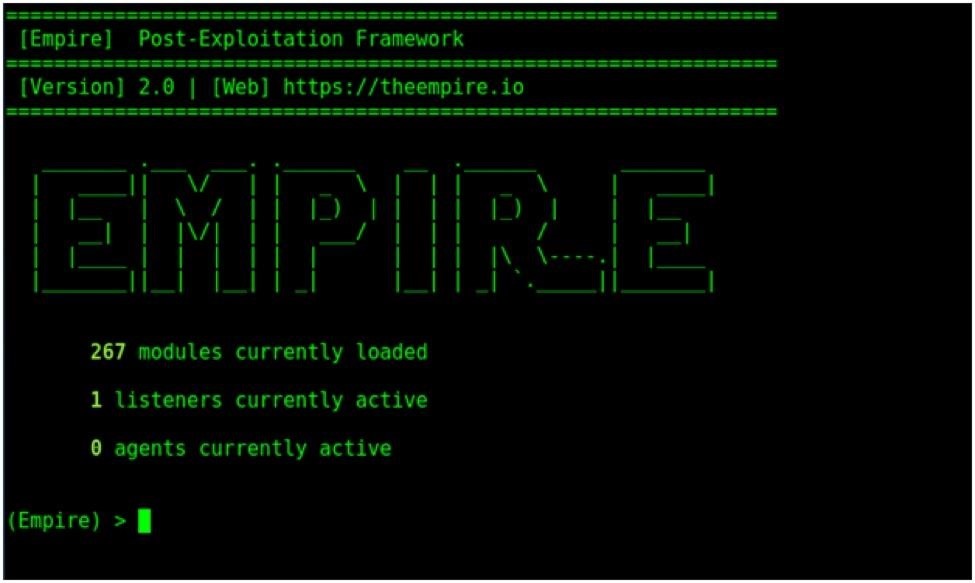
One important thing to remember is that Empire is case sensitive. For example, in the screenshot below, I am setting the "Name" value of our listener. "Name" and "name" are different in Empire, and it will give you an error if they are used incorrectly, as they cannot be used interchangeably.



When all options are set, we can start a listener using the **execute** command.



Once we go back to the main menu, we can see that our listener is currently active.



Step 4 Using Stagers

Stagers in Empire are used to set the stage for the post-exploitation activities. They are similar to payloads, which are used to create a connection back to Empire. The stagers can be accessed using the **usestager** command as shown below.

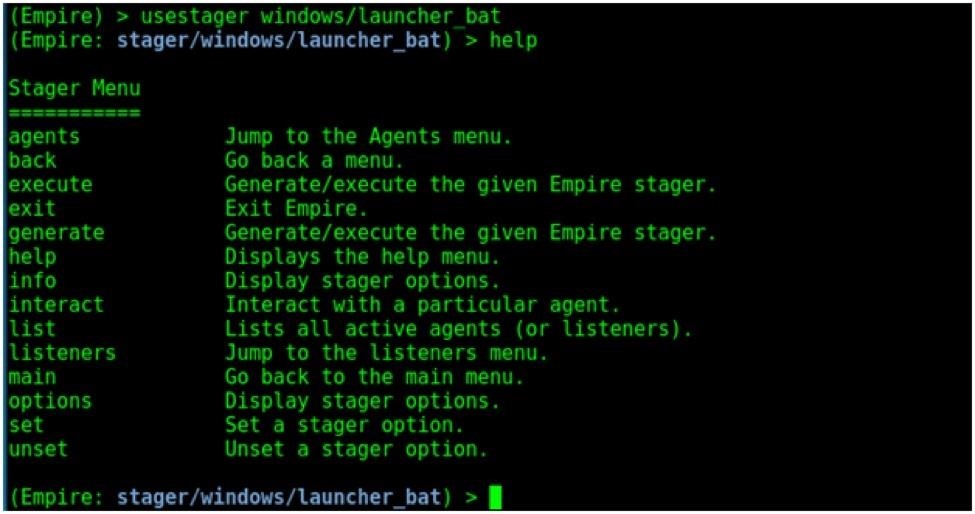
**Don't Miss:** [**How to Use Payloads with Metasploit**](../../../../docs/Technology/Hacking/ExploitDatabase/%20Metasploit.pdf)

Type the **usestager** and then use the tab completion to see all the available stagers.



We will learn about different stagers in an upcoming section. First, let's take a look at how to set up a stager.  
Let's start the "launcher\_bat" stager as an example.

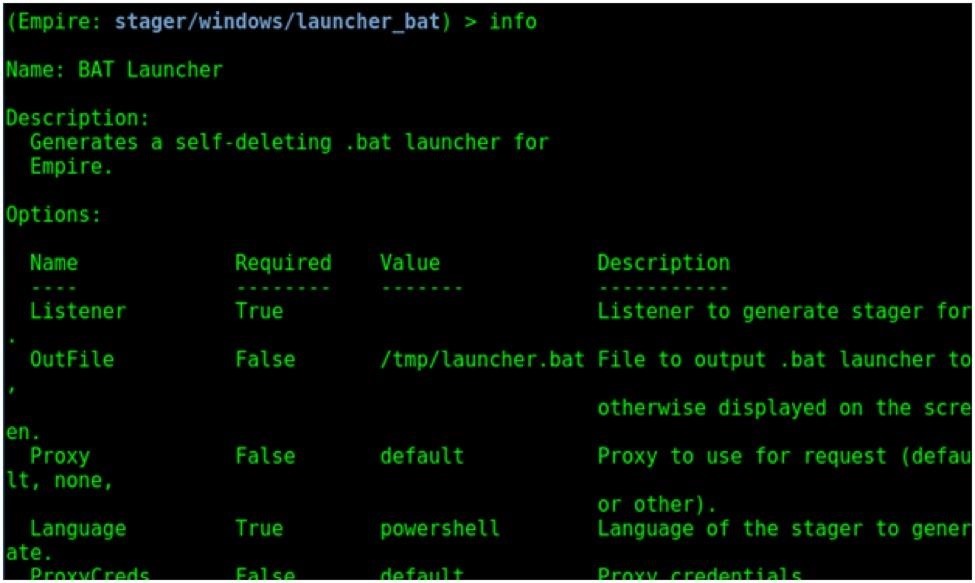
Type the **usestager windows/launcher\_bat** command to load the stager.



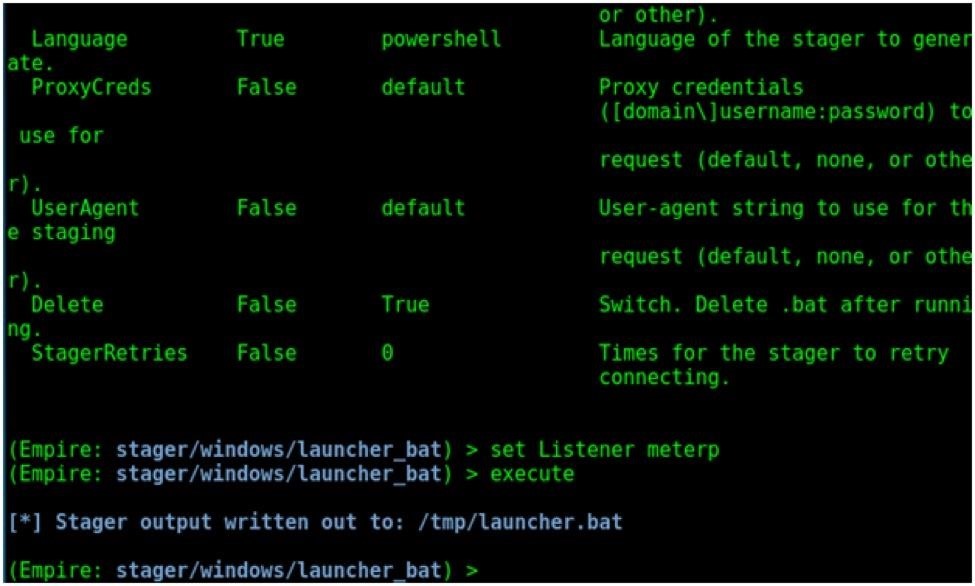
Type the **help** command to have a look at the stager menu.

* **agents** - Will allow you to jump directly to agents menu.
* **back & main** – Will take you back to the main menu.
* **exit** – Will exit from Empire.
* **help**- Will display help menu as shown in the above image.
* **info**- Will display information about the active listener.
* **kill**- Is used to kill a particular listener.
* **execute or generate** – Will execute or generate the stager.
* **interact** – Is used to interact with a particular agent (normally used when there are multiple listeners).
* **list** - Will list all the active listeners or agents.
* **options**- Used to see all the options we need to set for the particular agent.
* **set and unset** – Used to set and unset values to particular options, respectively.
* **listeners** - Used to jump to listeners menu.

We can get more information about this particular stager by using the **info** command. As you can see in the info, it creates a self-deleting batch file.



We need to set a listener in order for the stager to be able to communicate with Empire. In the last step, we have already created a listener. Let us set this listener for our "launcher\_bat" stager.

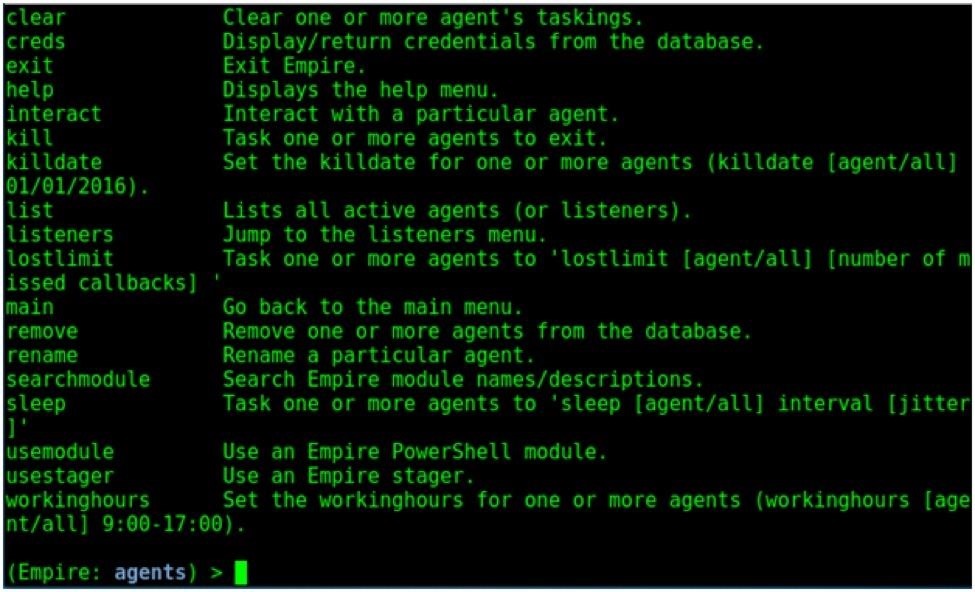
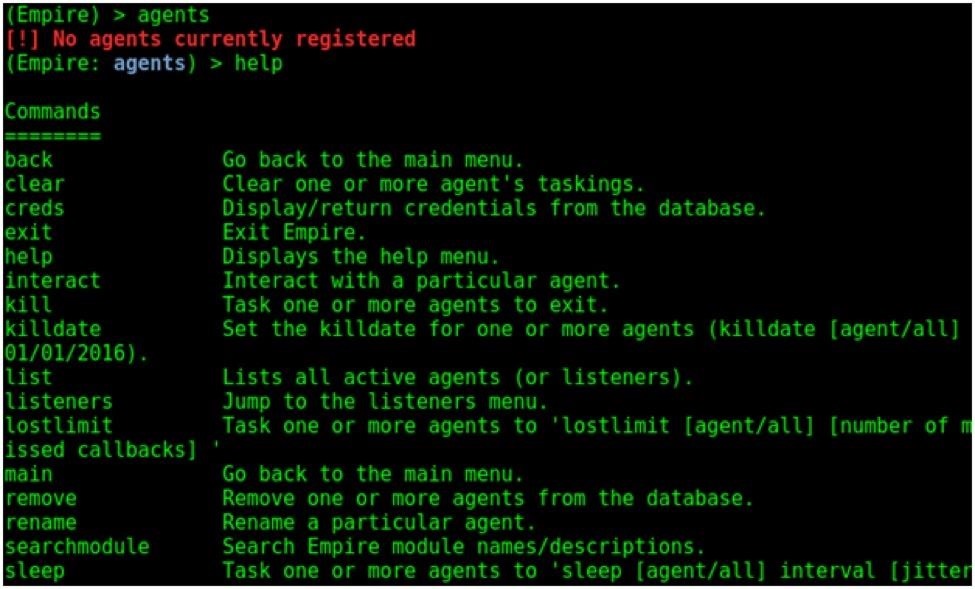


We can do this using **set Listener meterp** command. Type the **execute** command to generate the stager. The stager is created in the "tmp" folder as indicated by the output shown above in blue.

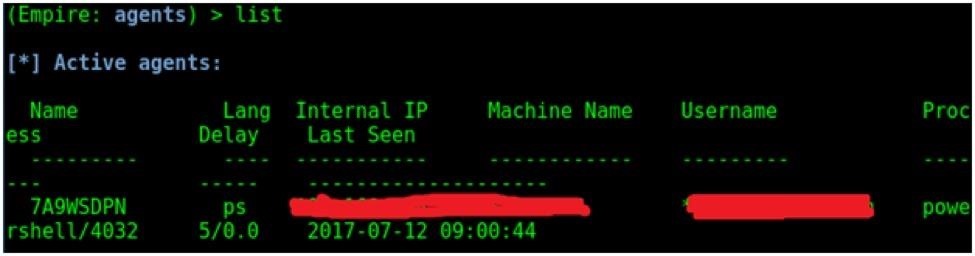
Step 5 Using Agents

When we send the stager to our target system and the machine engages with it, we get a reverse connection back. This is known as an agent.

The Agents menu can be accessed using **agents** command as shown below. But, as is stated in the red output, we do not currently have any agents registered. That is just around the corner.

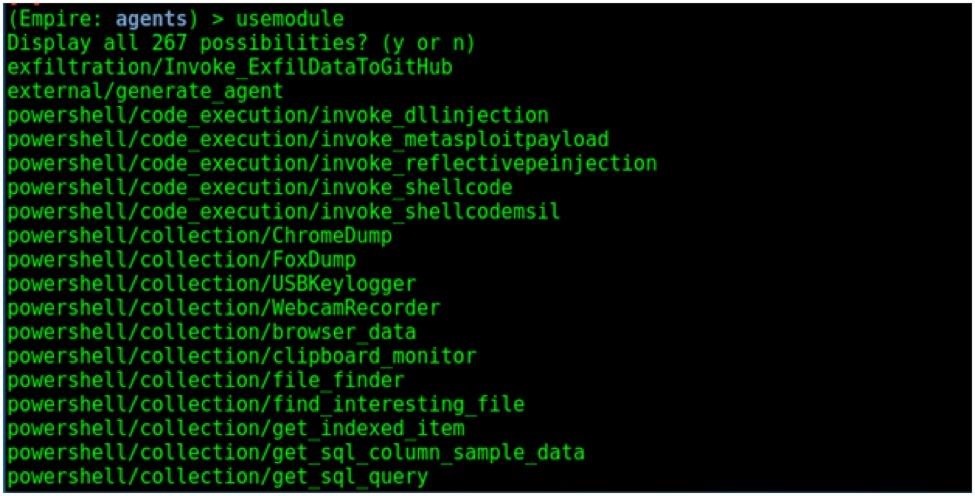


The output of the **help** command is shown above. It will display all the commands we can use when an agent establishes a connection with Empire. For example, typing the **list** command will show all the active agents we have, as shown below.

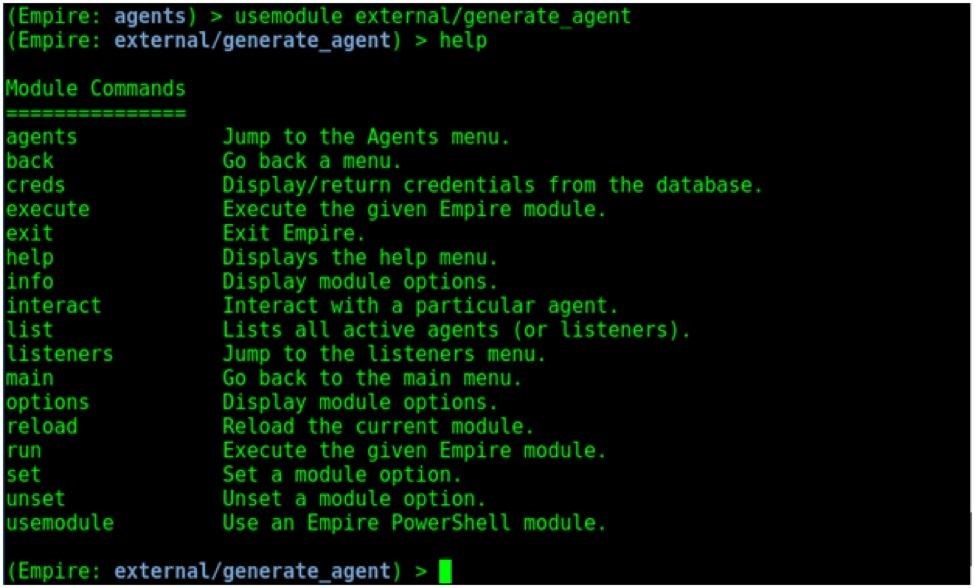


Step 6 Using Modules

Modules in Empire are used to perform specific functions. We can access modules using the **usemodule** command. Type **usemodule** *<Space>* and then use tab completion to see all the modules.

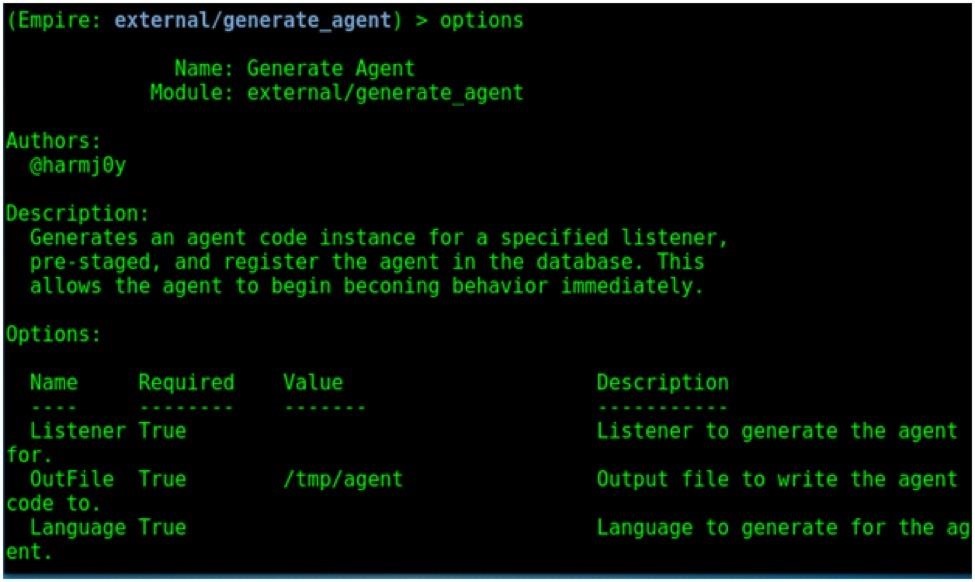


We will learn more about different modules in a later tutorial. First, let's take a look at how to use modules in Empire. Let's use the "external/generate\_agent" as an example. Type **usemodule external/generate\_agent** to load the module. Once the required module is loaded, type **help** to see all the commands we can use with the module.



* **agents** - Will allow you to jump directly to agents menu.
* **back & main** – Will take you back to the main menu
* **exit** – Will exit from Empire.
* **help** – Will display help menu as shown in the above image.
* **info** – Will display information about the active listener.
* **kill** – Is used to kill a particular listener.
* **execute or run** – Will execute the selected module.
* **interact** – Is used to interact with a particular agent (normally used when there are multiple listeners).
* **list** – Will list all the active listeners or agents.
* **options** – Is used to see all the options we need to set for the particular agent.
* **set and unset** – Used to set and unset values for particular options.
* **listeners** – Used to jump to listeners menu.
* **reload** – Will reload the current module.

Type the **options** command to see the options required for the module.



Set the required options using the **set** command, and when complete, use the **execute** command to generate the module.



We will get into more detail about Empire in the upcoming sections. These are the first steps in getting Empire up and running, so stay tuned for more! You can leave any questions in the comments below.