**Escalada de privilegios para el estudio de un keylogger y explotación de sistemas**



Daniel Escaño Hernández CET Ciberseguridad

# 

# **1. Índice:**

[**1. Índice:**](#_4jq84lualx9d) **1**

[**2. Práctica 2-3**](#_ofiic1av8ddq) **2**

[**2.1 Exploit EternalBlue y DoublePulsar para SMB y RDP de Windows**](#_5d38uxjyswtl) **2**

[**2.2 Comprobaciones previas al objetivo Windows**](#_ylx06qnd4y44) **3**

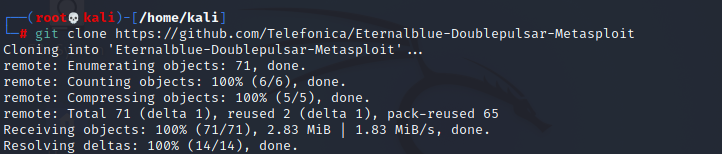
[**2.3 Comandos básicos de Meterpreter y Escalada de Privilegios**](#_hzvd5m4vedi1) **6**

[**2.4 Infección con keylogger**](#_myznhl1h199e) **9**

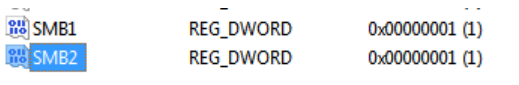
# **2. Práctica 2-3**

### **2.1 Exploit EternalBlue y DoublePulsar para SMB y RDP de Windows**

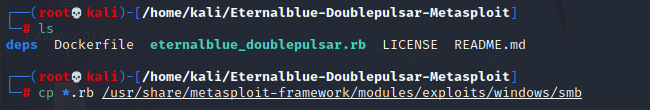
Descargamos los archivos necesarios



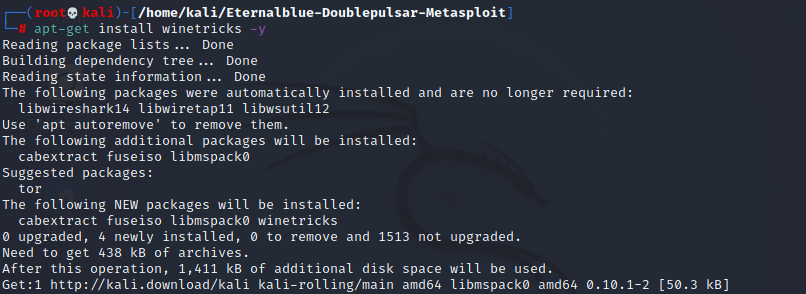
Comprobamos que los protocolos SMB1 y SMB2 se encuentran activos en la máquina Windows

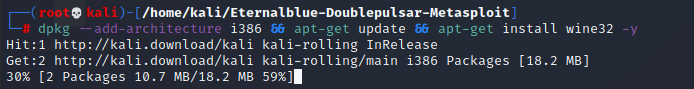


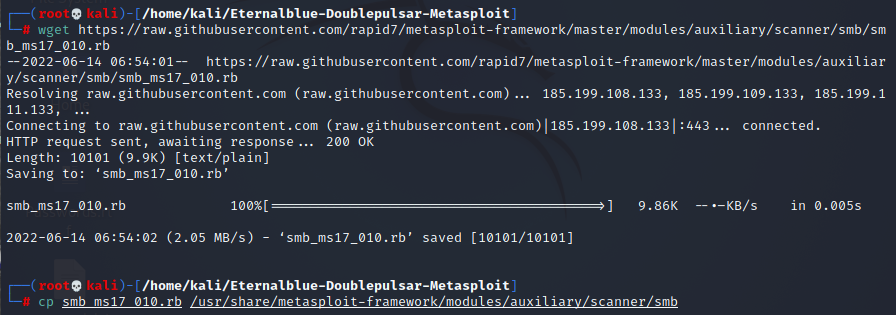
Copiamos eternalblue para poder utilizarlo en el framework



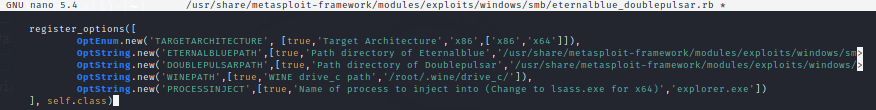
Descargamos dependencias y prerrequisitos





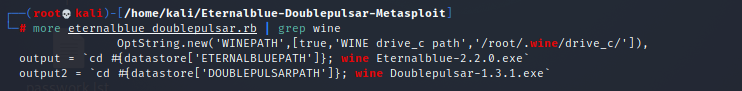


Modificamos el archivo de configuración



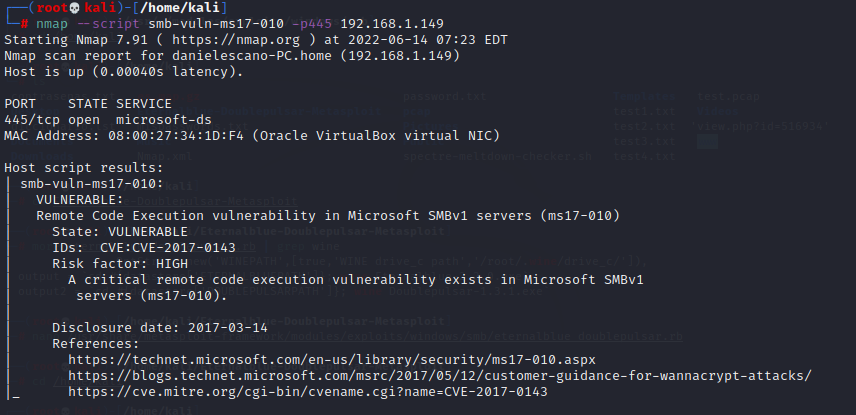
### **2.2 Comprobaciones previas al objetivo Windows**

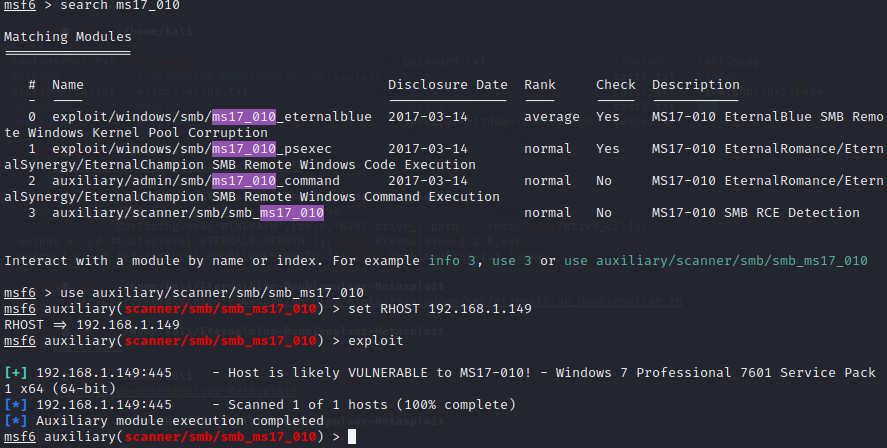
Procedemos a configurar Wine



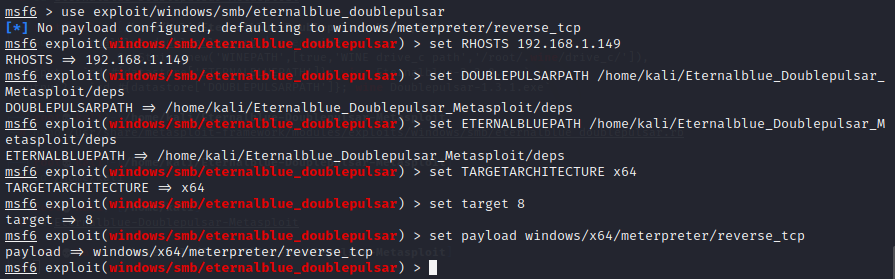


Comprobamos si la máquina es vulnerable de diferentes formas

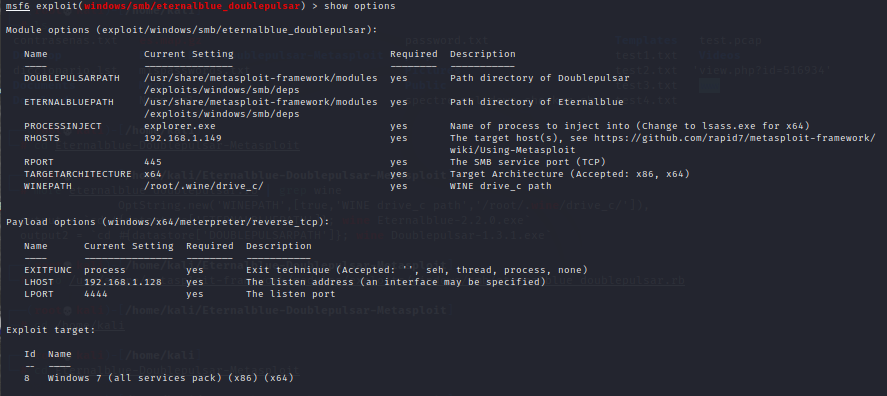




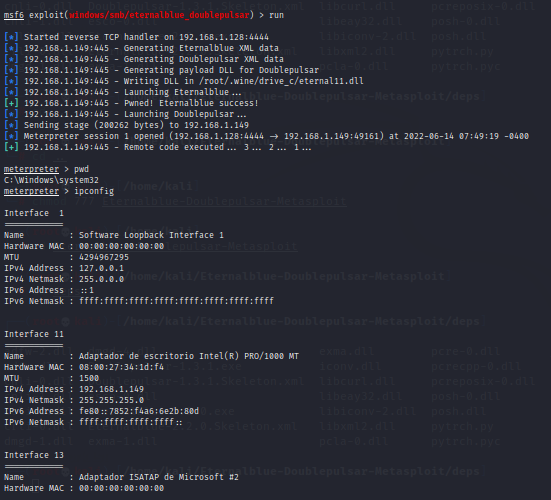
Pasamos a modo ataque y configuramos los parámetros necesarios



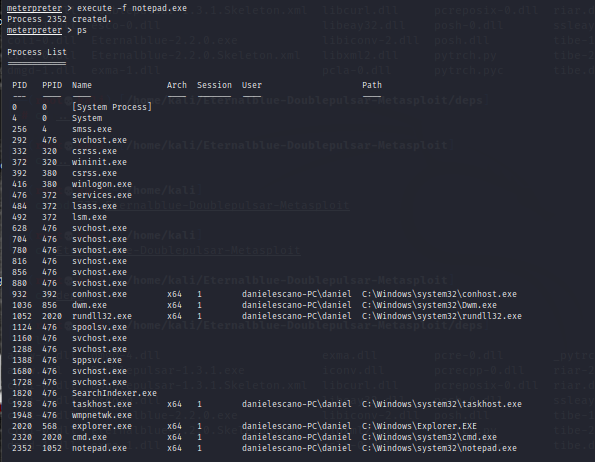
La opción show options, nos permite ver un resumen de los parámetros empleados



Ejecutamos el ataque y realizamos diferentes comprobaciones

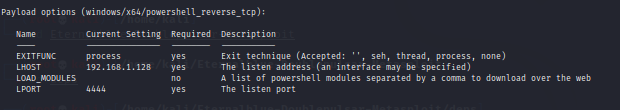


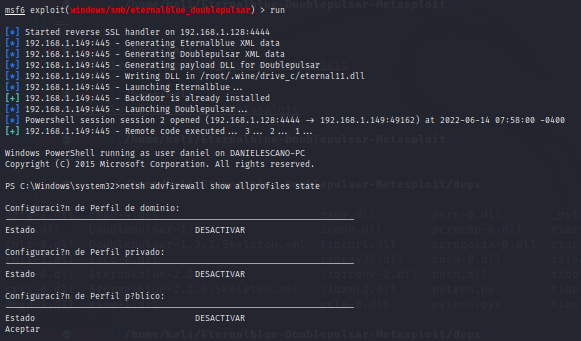




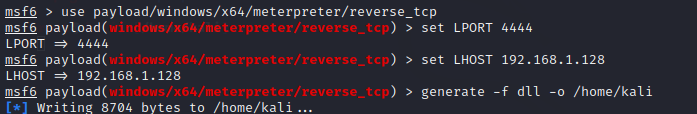
### **2.3 Comandos básicos de Meterpreter y Escalada de Privilegios**

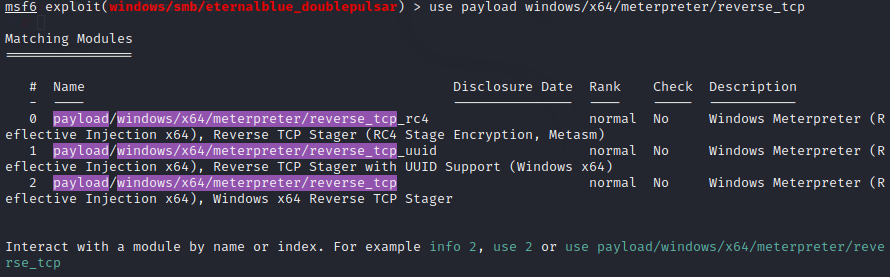
Modificamos el ataque para que nos aparezca una powershell y comprobamos diferentes parámetros del firewall



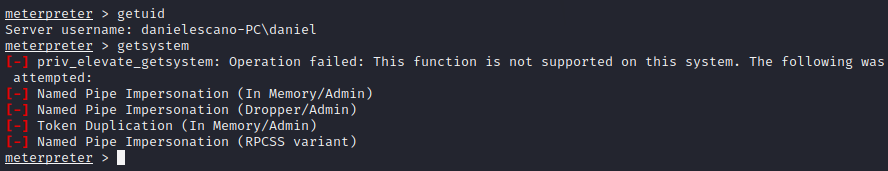


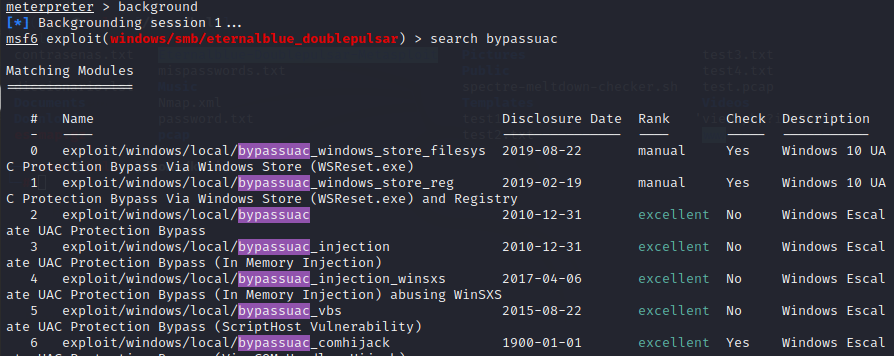
Generamos un dll y procedemos a crear el siguiente ataque impersonador.

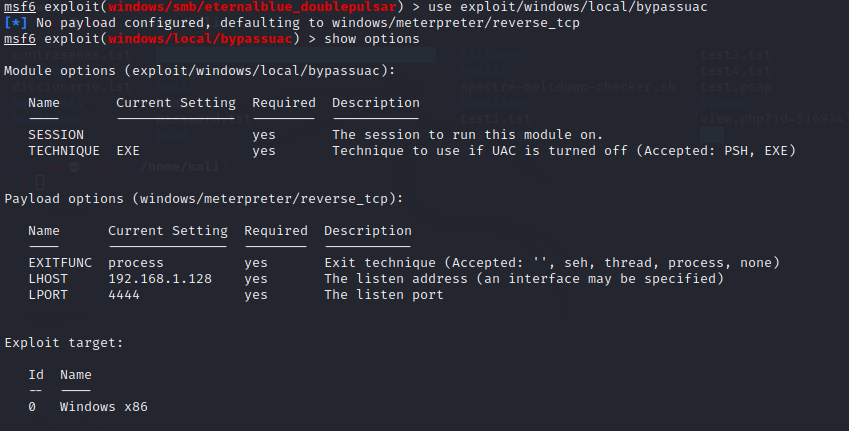


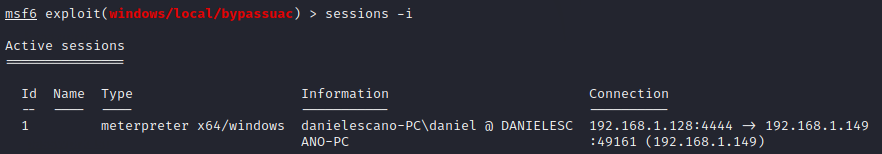


Como podemos observar no funciona en este momento, procedemos a configurar los parámetros necesarios:

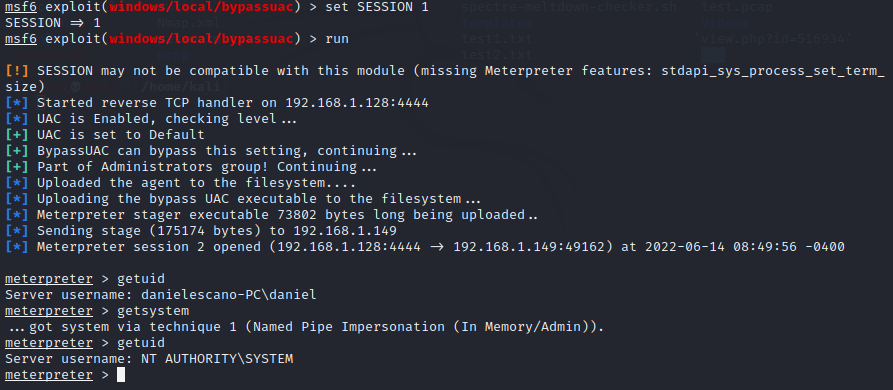


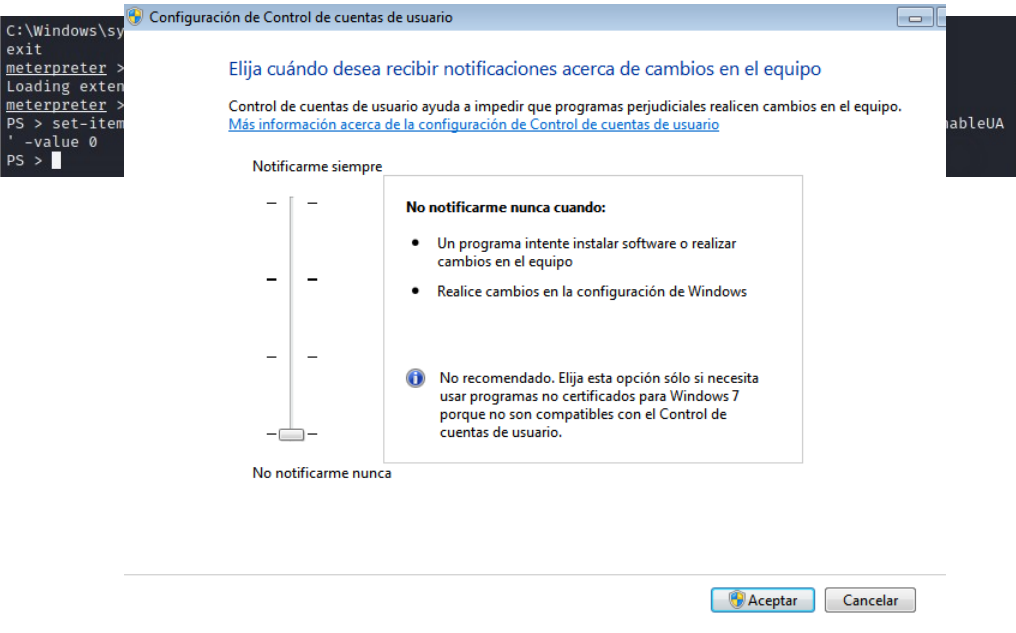






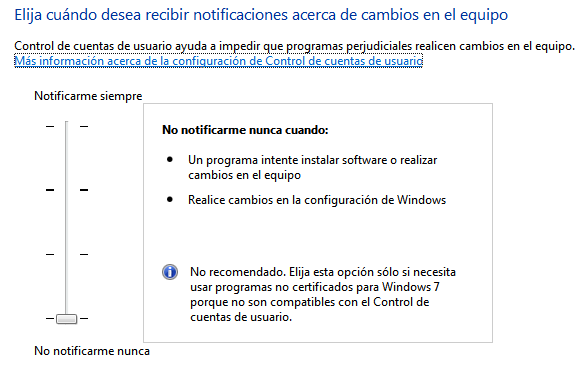
Asignamos a la sesión deseada, ejecutamos el ataque y comprobamos desactivando las políticas de seguridad UAC:



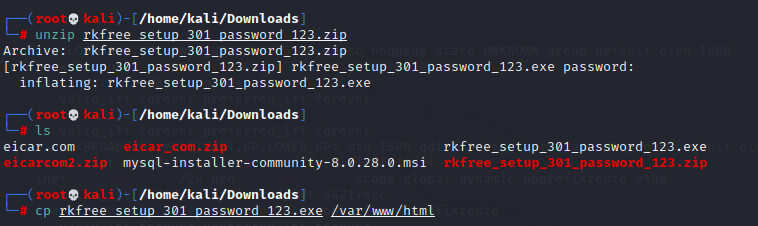


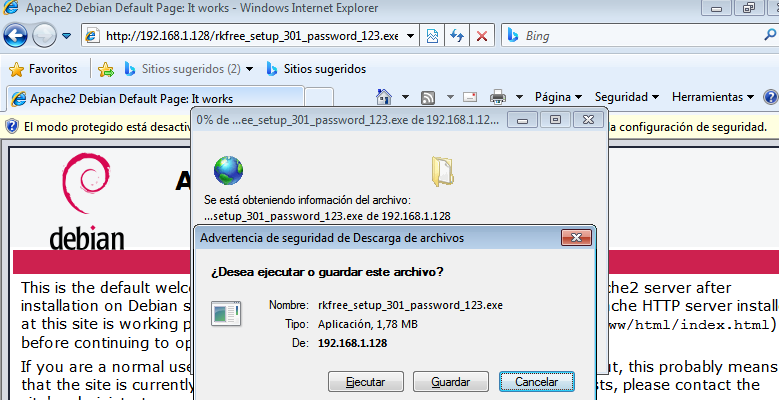
### **2.4 Infección con keylogger**



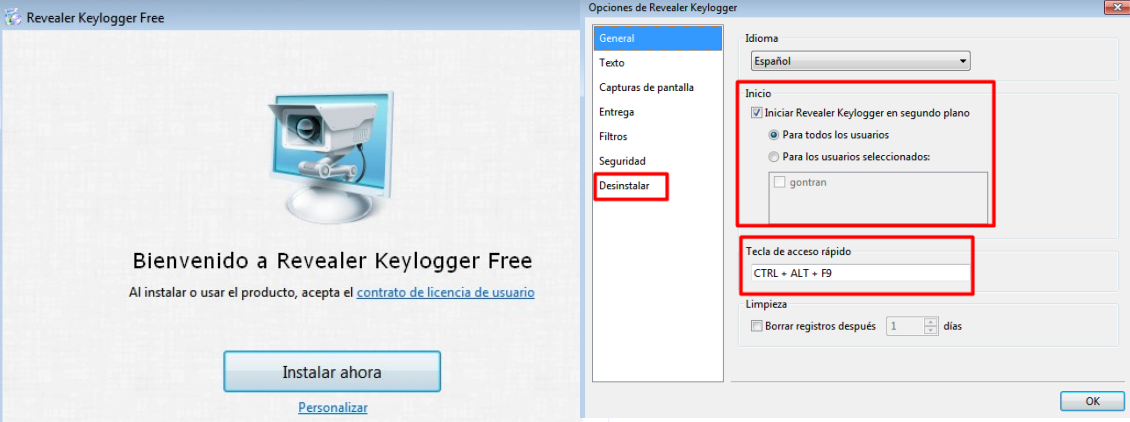


Realizaremos una infección de un keylogger a través de nuestro servidor apache, movemos el archivo a nuestro directorio configurado para apache.





Descargamos el fichero y procedemos a su instalación



Por último comprobaremos si un antivirus común, es capaz de detectar dicho keylogger, en este caso panda cloud cleaner, procedemos a su instalación y examen

