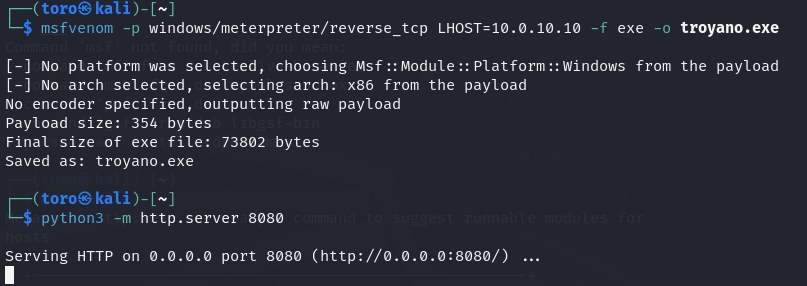
EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN WINDOWS II Prerrequisitos

Kali Linux

Windowsploitable LPE

Ejercicio - SharpUp, Reg query, Msfvenom y Metasploit

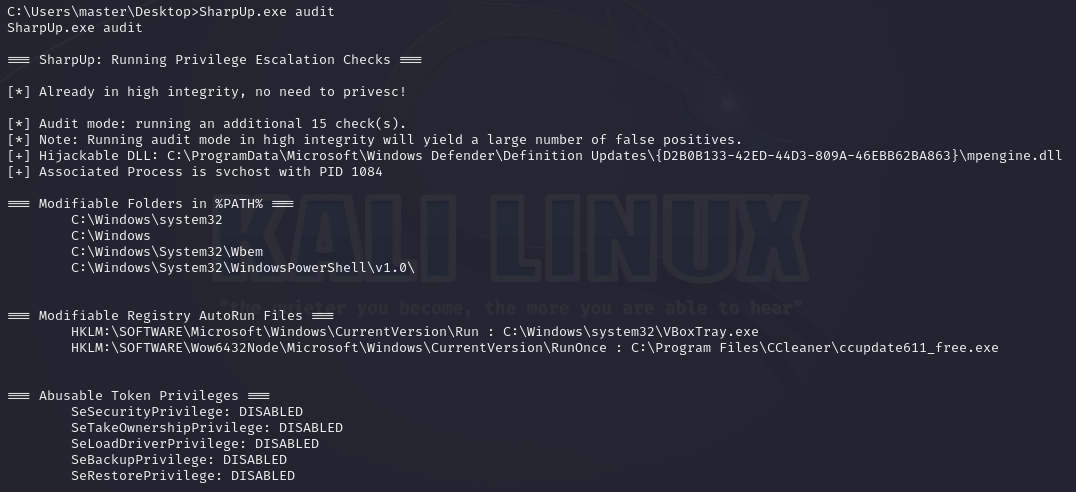
Crear un troyano y transferirlo al escritorio del usuario user en el sistema Windowsploitable LPE.



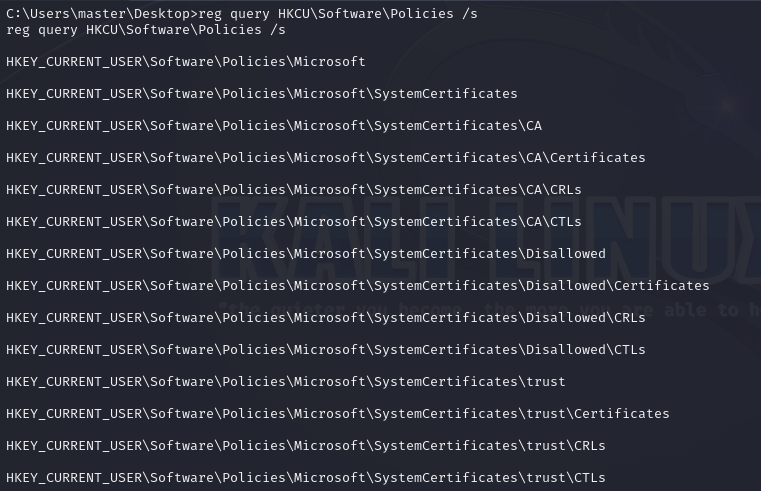
Utiliza un exploit multi/handler para obtener un meterpreter reverso.



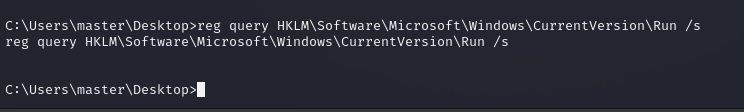
Explotar los permisos del usuario user en las claves de registro usando SharpUp.exe para obtener información de las mismas.



También, comprobar los valores de las claves de registro por querys en shell. Explicar los resultados.



HKCU\Software\Policies: Esta clave contiene políticas aplicadas al usuario actual. Si tenemos permisos para modificar estas claves, podríamos agregar un valor para ejecutar un script o programa malicioso al iniciar sesión.



HKLM\Software\Microsoft\Windows\CurrentVersion\Run: Esta clave se utiliza para ejecutar programas al iniciar el sistema. Si tenemos permisos para modificar estas claves, podríamos agregar nuestro troyano para que se ejecute al iniciar el sistema.

Crear un troyano de tipo instalador .msi y transferir al sistema en alguna ruta donde tengamos permisos.



Ejecutar el instalador en modo silencioso y demostrar obtener sesión con privilegios.

