EJERCICIOS EVASIÓN DE WINDOWS UAC

Prerrequisitos

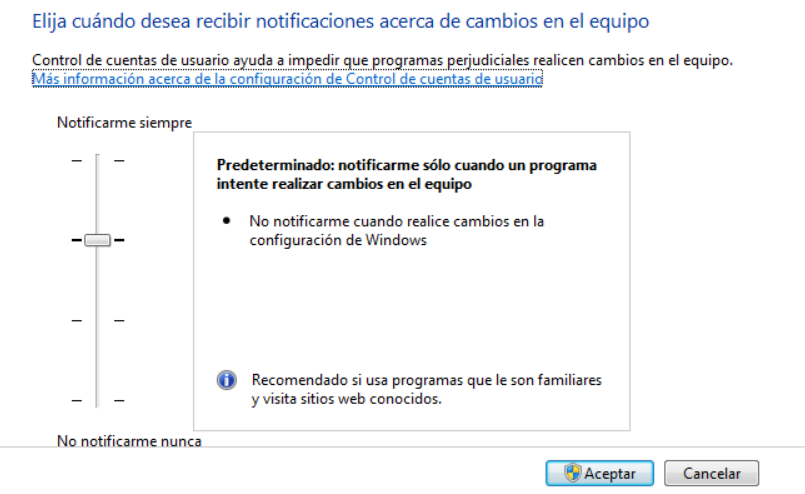
Kali Linux

Windowsploitable LPE

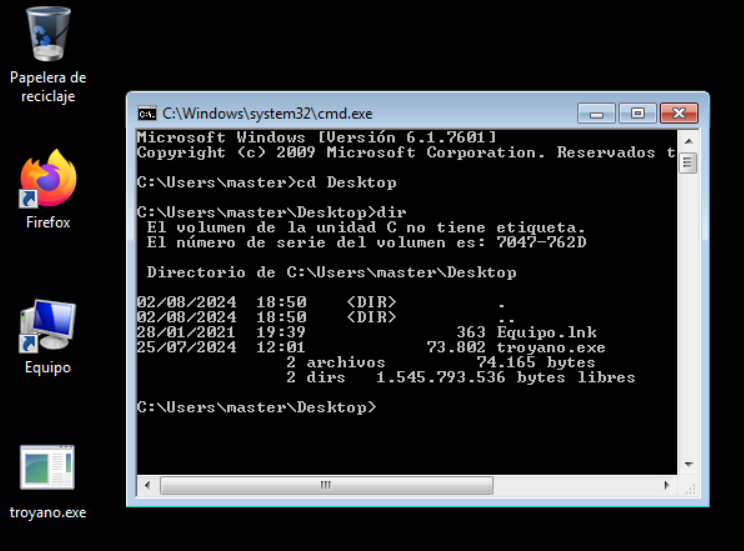
Windows 10 Evasion

Ejercicio 1 - Metasploit y Windows UAC

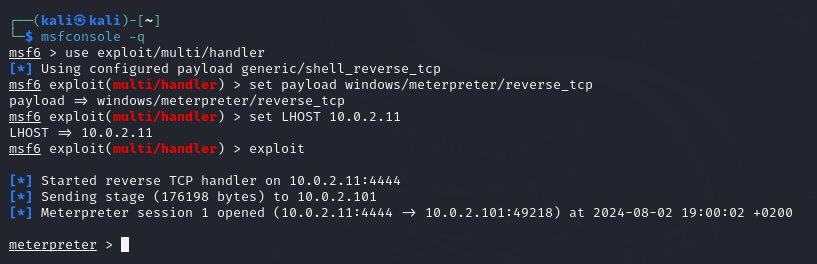
Entrar en el entorno gráfico de Windowsploitable LPE con el usuario master y habilitar Windows UAC eligiendo nivel predeterminado.



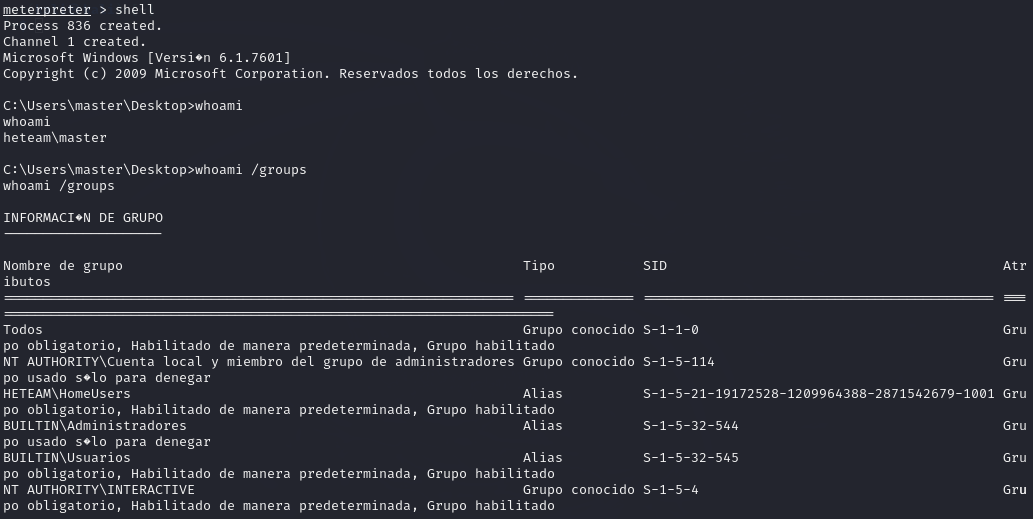
Crear un troyano y transferirlo al escritorio del usuario master en el sistema Windowsploitable LPE.



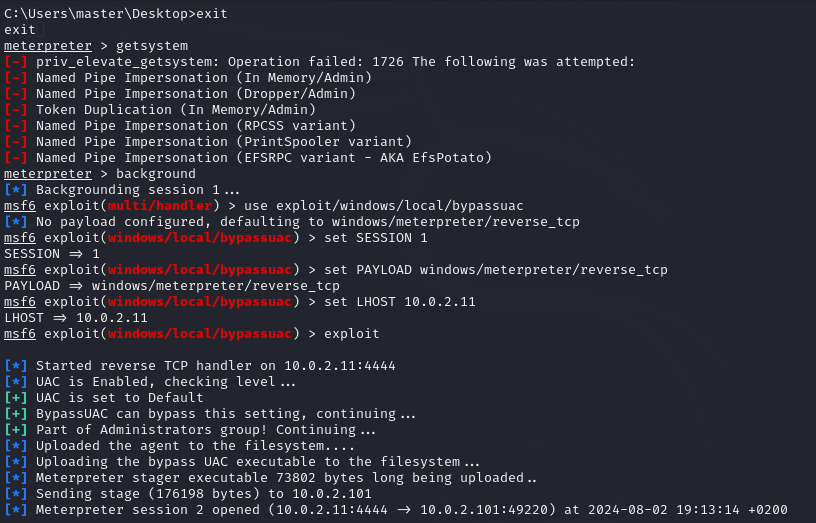
Utiliza un exploit multi/handler para obtener un meterpreter reverso.



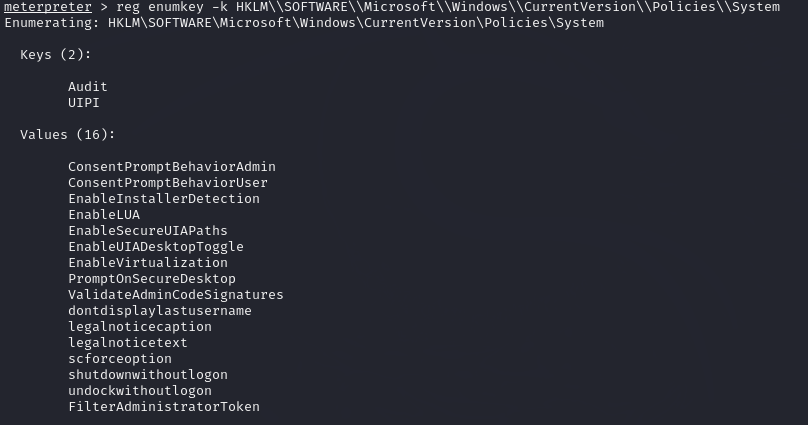
En la sesión, abrir una shell y comprobar los permisos del usuario master y los grupos a los que pertenece.

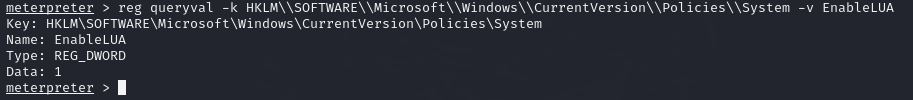


Intentar elevar privilegios a NT Authority\System con comando de meterpreter. En caso de no funcionar, utilizar un módulo de bypass para evadir el UAC y conseguir así una nueva sesión con privilegios elevados.



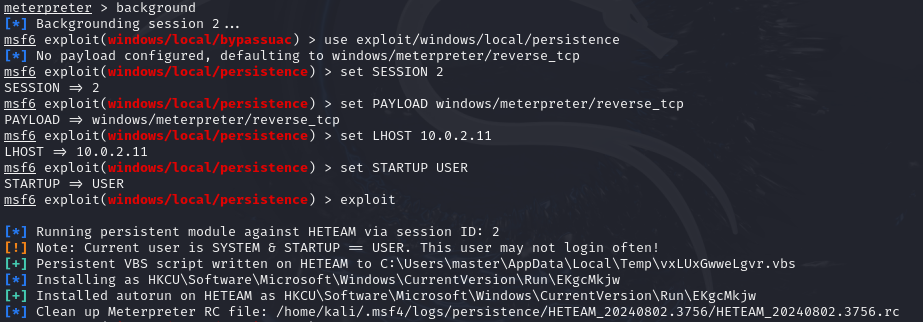
En esta nueva sesión, realizar una elevación a NT Authority\System con comando de meterpreter. Consultar la clave de registro de políticas del sistema y después la subclave de Windows UAC explicando los resultados obtenidos.

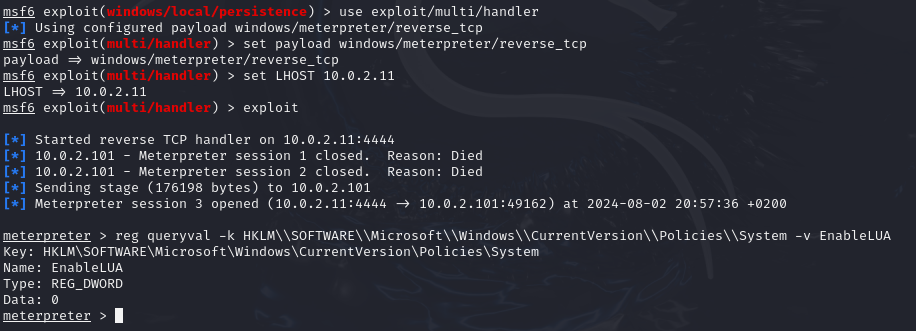




si EnableLUA está configurado en 1, UAC está habilitado

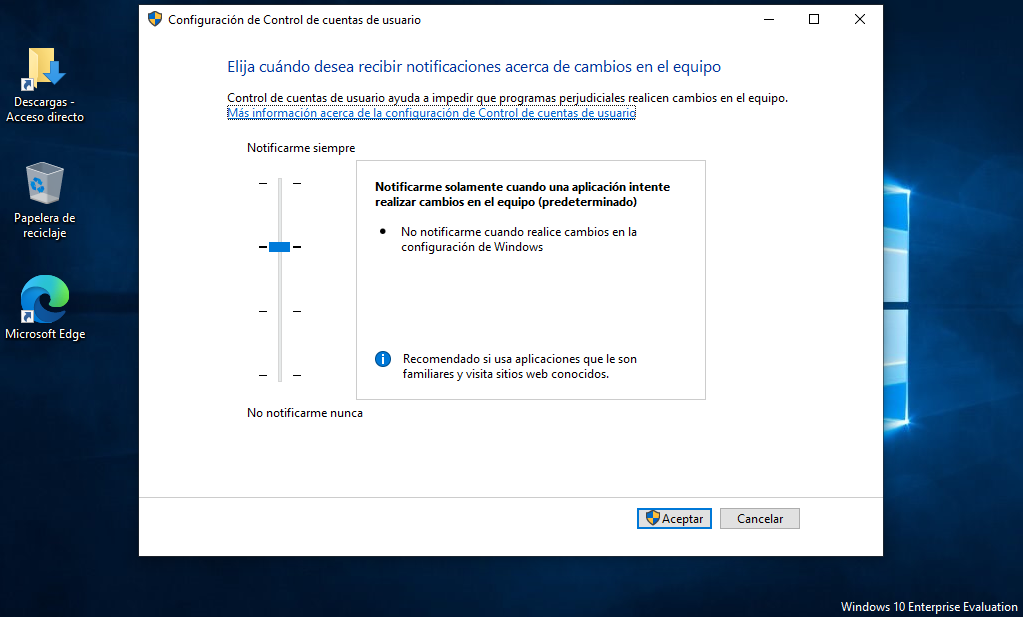
Deshabilitar la subclave de registro de Windows UAC y crear un backdoor persistente para comprobar en la sesión obtenida si el valor quedó almacenado de forma permanente en el registro del sistema.



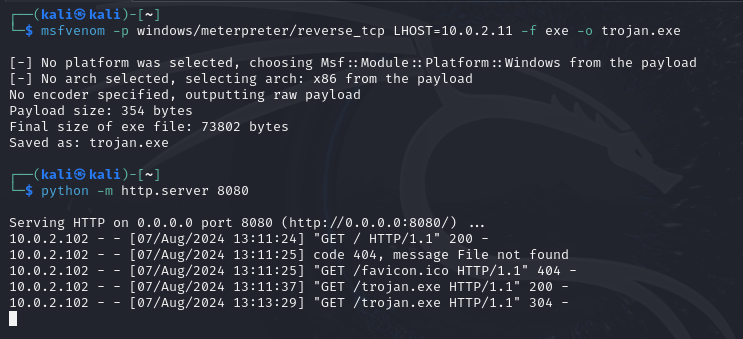


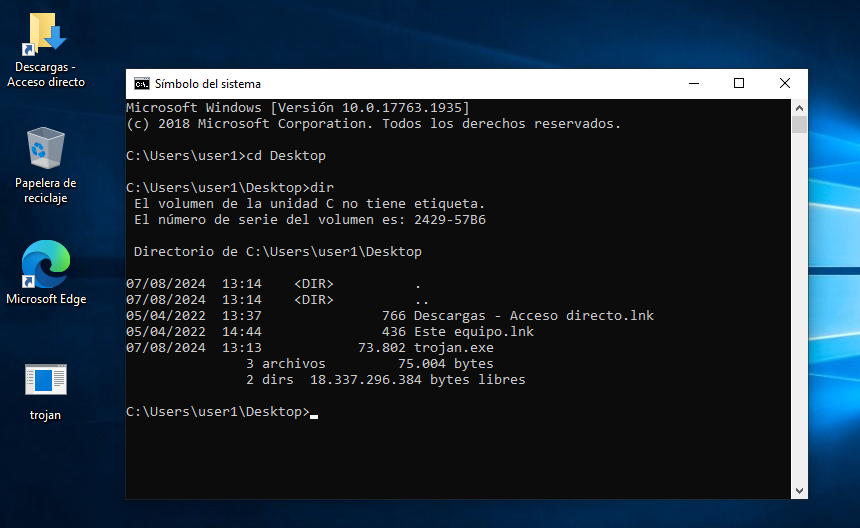
Ejercicio 2 - Metasploit y Windows UAC

Entrar en el entorno gráfico de Windows 10 Evasion con el usuario user1 y habilitar Windows UAC eligiendo nivel predeterminado.

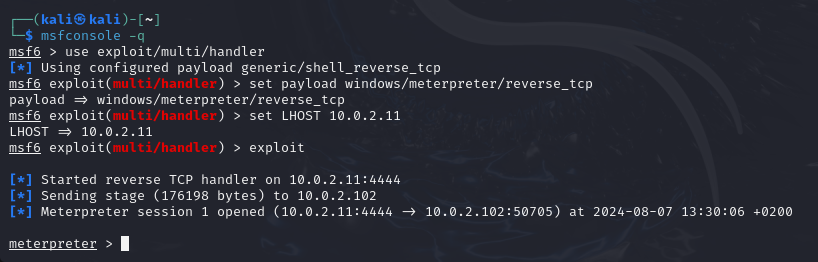


Crear un troyano y transferirlo al escritorio del usuario user1 en el sistema Windows 10 Evasion.

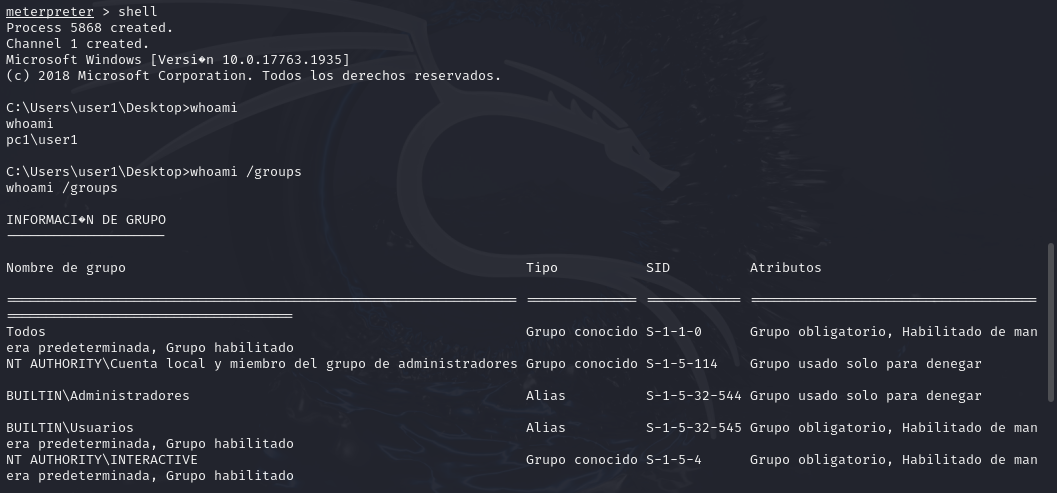




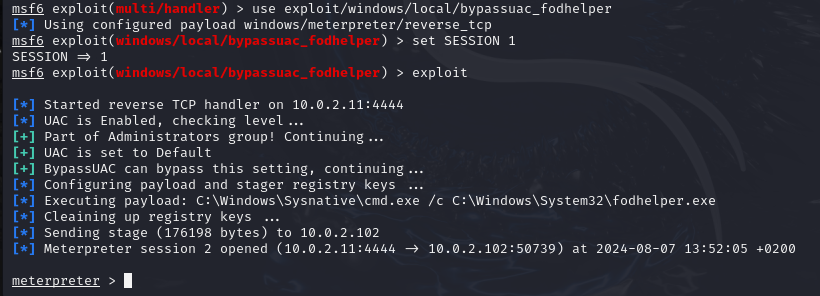
Utiliza un exploit multi/handler para obtener un meterpreter reverso.



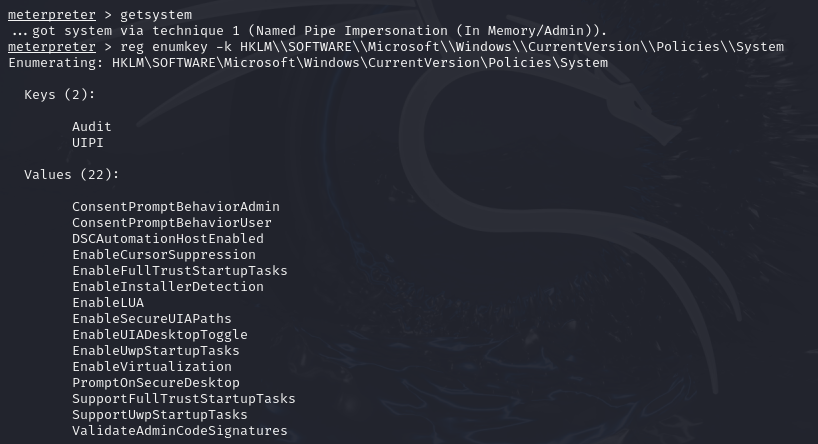
En la sesión, abrir una shell y comprobar los permisos del usuario user1 y los grupos a los que pertenece.

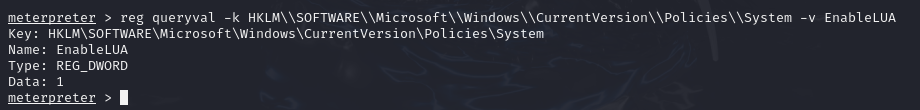


Intentar elevar privilegios a NT Authority\System con comando de meterpreter. En caso de no funcionar, utilizar un módulo de bypass para evadir el UAC y conseguir así una nueva sesión con privilegios elevados.



En esta nueva sesión, realizar una elevación a NT Authority\System con comando de meterpreter. Consultar la clave de registro de políticas del sistema y después la subclave de Windows UAC explicando los resultados obtenidos.





Clave de registro de políticas del sistema: indica todos los valores que incluirán configuraciones importantes relacionadas con la política de seguridad y comportamiento del sistema.

Subclave de Windows UAC: indica si UAC está habilitado (1) o deshabilitado (0). UAC es una característica de seguridad que ayuda a prevenir cambios no autorizados en el sistema operativo.