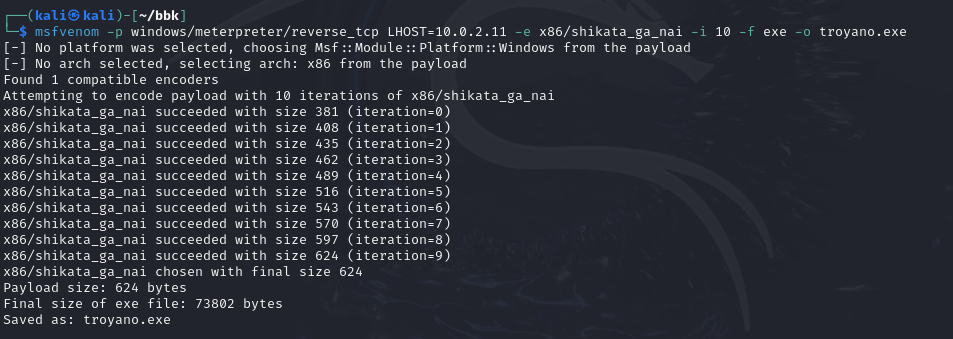
EJERCICIOS INTRODUCCIÓN A LA EVASIÓN DE DEFENSAS Prerrequisitos

Kali Linux

Windows 8 Evasion

Ejercicio - Msfvenom y metasploit

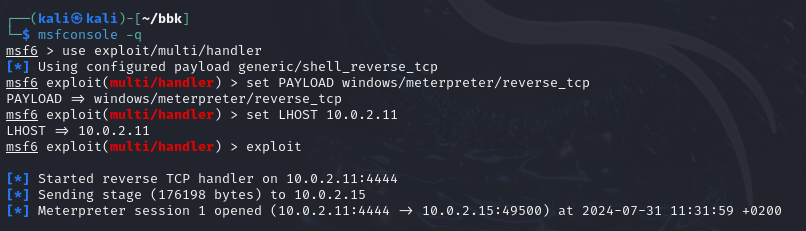
Crear un troyano para Windows que tenga menos de 30 detecciones en VirusTotal con técnicas como los encoders y las iteraciones.



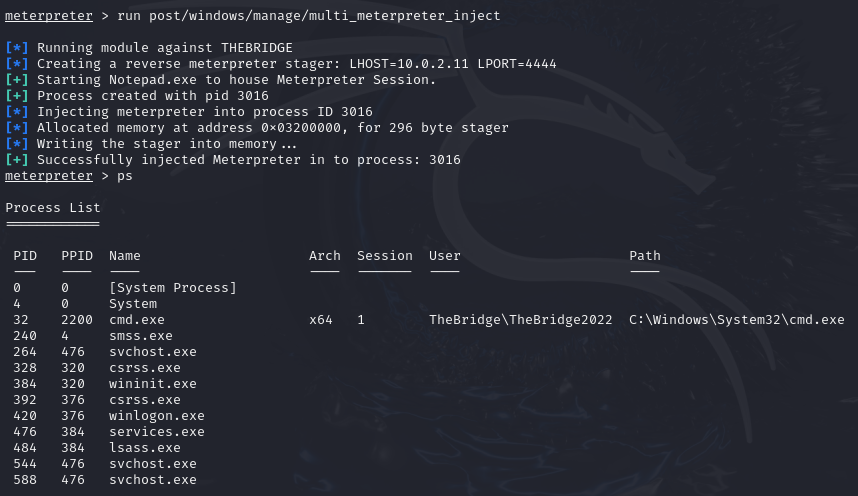
Transferir el troyano al escritorio del sistema Windows 8 Evasion.



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



Usar el módulo multi\_meterpreter\_inject para inyectar el payload en al menos dos nuevos procesos y así favorecer la migración.



Migrar a alguno de los procesos creados y utilizar comando de meterpreter para el borrado de logs.



En caso de no tener éxito, elevar privilegios y después realizar el borrado de logs.

