EJERCICIOS INGENIERÍA SOCIAL Y HERRAMIENTAS DE EVASIÓN

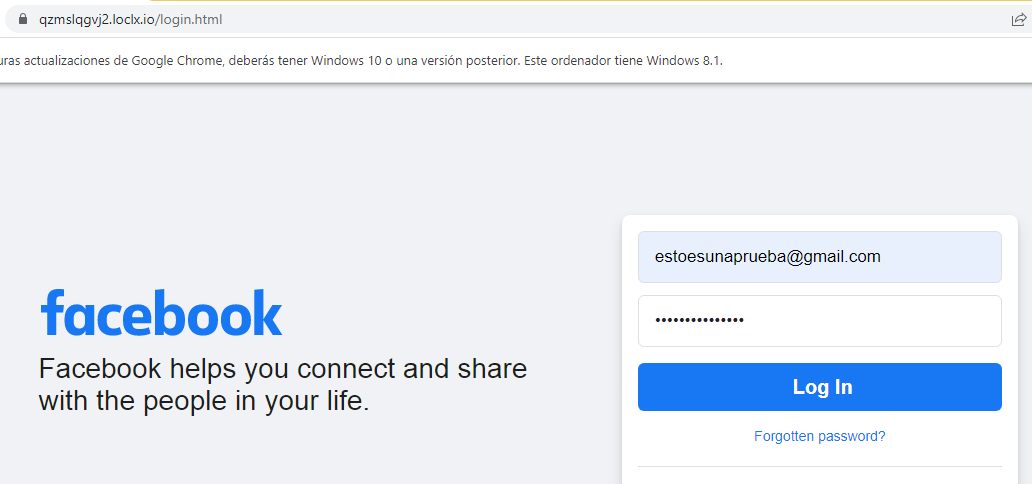
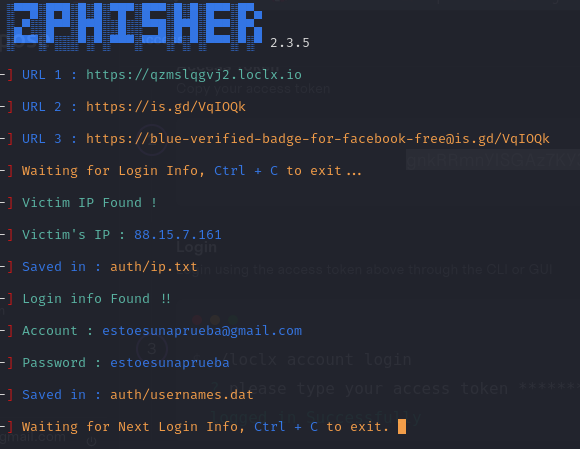
Prerrequisitos

Kali Linux

Windows 8 Evasion

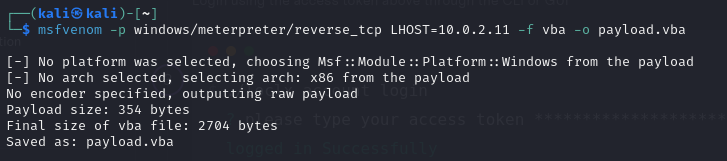
Ejercicio 1 - Zphisher y Localxpose

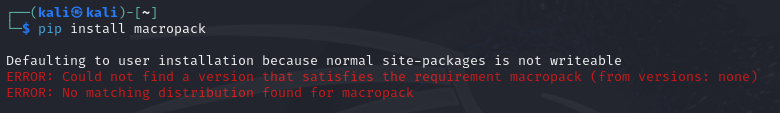
Realizar un ataque de phishing contra el sistema Windows 8 Evasion para obtener credenciales de Facebook.



Ejercicio 2 - Msfvenom y Macropack

Crear un troyano con Msfvenom de tipo Visual Basic Application para despues convertirlo en un documento Word con macros maliciosas.

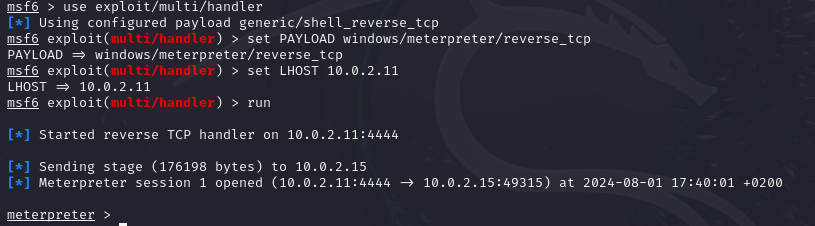




No se puede instalar macropack, de haberlo echo lo habría convertido con:

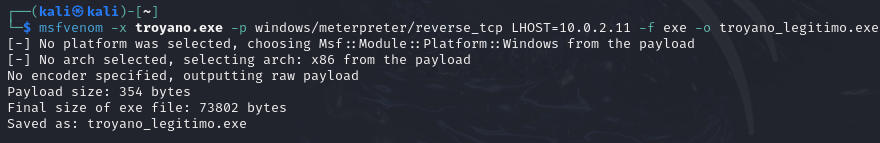
macropack --input payload.vba --output troyano.docm --template prueba.docx

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

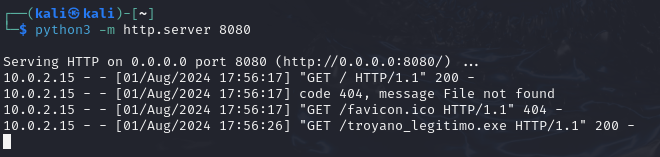


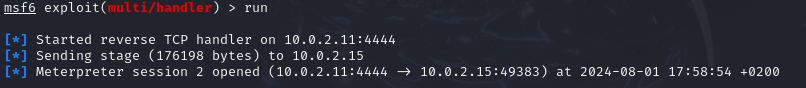
Ejercicio 3 - Metasploit y Msfvenom

A partir de la sesión obtenida anteriormente, crear un troyano que mantenga su comportamiento habitual usando algún archivo ejecutable legítimo del sistema Windows 8 Evasion con Msfvenom.



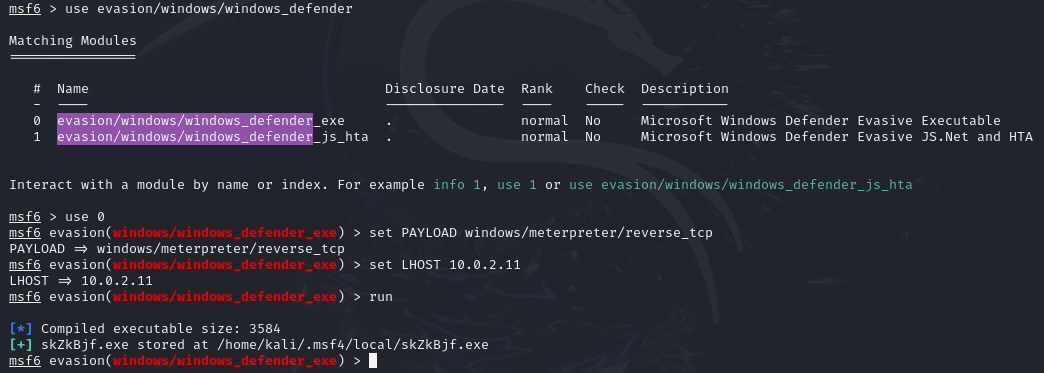
Demostrar que mantiene su comportamiento habitual ejecutándolo en el sistema Windows 8 Evasion y que crea una nueva sesión mediante un exploit multi/handler para obtener otro meterpreter reverso.





Ejercicio 4 - Metasploit

Crear un troyano que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal usando el módulo de evasion de metasploit windows\_defender.



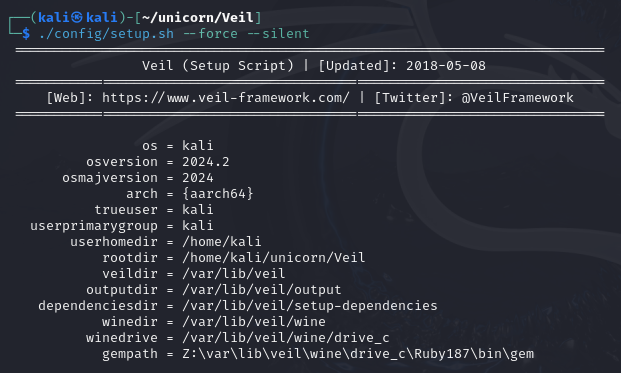
Ejercicio 5 - Unicorn

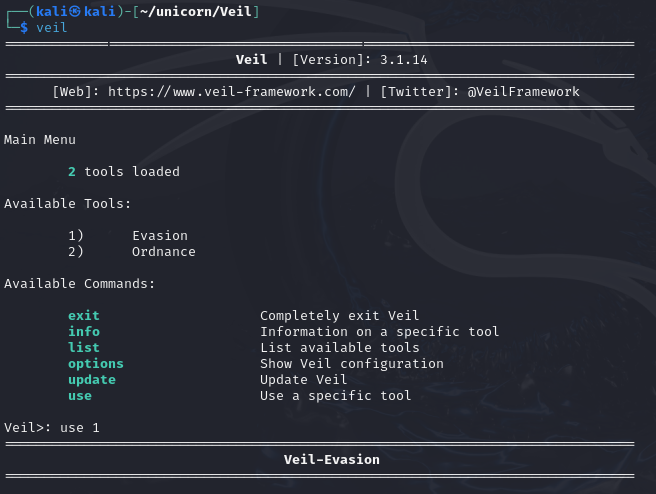
Crear un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con Unicorn.

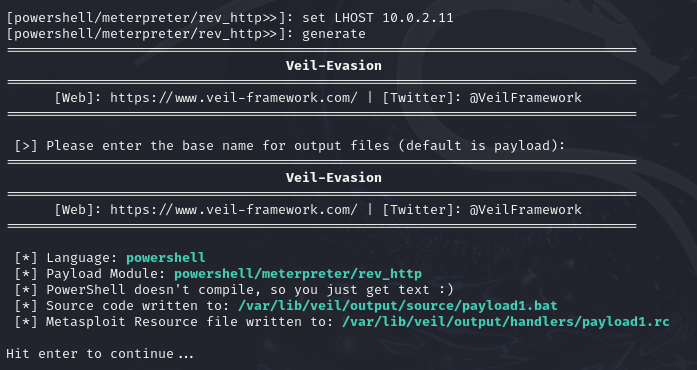




Ejercicio 6 - Veil

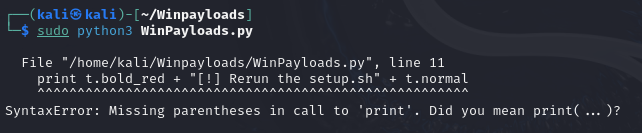
Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con Veil.





Ejercicio 7 - WinPayloads

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con WinPayloads.



No se puede ejecutar winpayloads, así que no puedo seguir…