Melvin Misael Joj Gil
0910-18-1946
Ingeniería de software

Herramientas para ingeniería inversa

¿Qué es la ingeniería inversa?

La ingeniería inversa es el proceso o técnica de descubrir los principios tecnológicos de un producto, herramienta, dispositivo o sistema.

Los productos más típicamente sometidos a esta técnica son los programas para ordenador, pero cualquier producto puede ser objeto de análisis de ingeniería inversa.

Se denomina así porque avanza en dirección opuesta a las tareas habituales de ingeniería, que consisten en utilizar datos técnicos para elaborar un producto determinado. (Revista Digital, 2019)

Herramientas

WINDBG

Este depurador es mantenido directamente por Microsoft y se incluye en Windows Driver Kit (WDK). Actualmente es considerada la herramienta de depuración de kernel más actualizada y poderosa y puede operar en modo kernel, aunque no cuenta con una interfaz muy accesible para sus nuevos usuarios.

IDA DISASSEMBLER

Esta herramienta cuenta con una versión gratuita y una de paga. La primera versión solo es compatible con x86, además de que no admite plugins. Por otra prte, la versión de pago puede usarse sin restricciones de arquitectura o plugins, lo que la hace una opción mucho mejor para los investigadores.

RADARE2

Acorde a los expertos en ingeniería inversa de malware, esta herramienta fue pensada originalmente como un editor hexadecimal, aunque eventualmente fue convertido en un marco completo para la depuración y desensamblado de toda clase de código, incluyendo software malicioso.

DETECT IT EASY (DIE)

Este es un excelente programa para identificar empacadores, además de contar con muchas otras funcionalidades como el cálculo de la entropía de las secciones de archivo.

EXEINFOPE

Este es un detector de empaquetadores y protectores muy funcional aunque con una interfaz bastante peculiar que puede llegar a ser difícil de entender. Aun así, el programa se actualiza de forma constante y está lleno de características interesantes para los expertos en ingeniería inversa de malware.

HXD

HxD es un miembro destacado de la familia de los editores hexadecimales, pues es una de las principales opciones para acceder a un disco duro, memoria o aplicación en modo binario. La herramienta es gratuita y se actualiza constantemente, además de que permite eliminar archivos de forma segura y compatibilidad con una versión portátil.

HIEW

Esta herramienta cuenta con una versión gratuita y una de paga y que recibe mantenimiento constante por parte de los desarrolladores. Los expertos en ingeniería inversa de malware mencionan que esta es una herramienta similar a Norton Commander, aunque la interfaz de usuario es un poco más compleja. (Noticias de seguridad informática, 2021)

Referencias

Revista Digital INESEM (28 de enero de 2019) *Recomendaciones para realizar el proceso de Ingeniería Inversa* https://revistadigital.inesem.es/informatica-y-tics/ingenieria-inversa/

Noticias de seguridad informática (28 de mayo de 2021) *Las 15 mejores herramientas de ingeniería inversa para el análisis de malware, software y tráfico de red* https://noticiasseguridad.com/tutoriales/las-15-mejores-herramientas-de-ingenieria-inversa-para-el-analisis-de-malware-software-y-trafico-de-red/