

27. Ingeniería inversa

Sunday, August 30, 2020 6:44 PM

La **ingeniería inversa** o **retro ingeniería** es el proceso llevado a cabo con el objetivo de obtener información o un diseño a partir de un producto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí y cuál fue el proceso de fabricación.

La ingeniería inversa de software (SRE) es la práctica de analizar un sistema de software, ya sea en su totalidad o en parte, para extraer información de diseño e implementación. Un escenario SRE típico implicaría un módulo de software que ha trabajado durante años y lleva varias reglas de un negocio en sus líneas de código; por desgracia, el código fuente de la aplicación se ha perdido - lo que queda es código "nativo" o "binario". Las habilidades de ingeniería inversa también se utilizan para detectar y neutralizar virus y malware, y para proteger la propiedad intelectual. Se necesitarán programadores informáticos competentes en SRE en caso de que los componentes de software como estos necesiten mantenerse, mejorarse o reutilizarse.








Herramientas para Ingeniería inversa de software: [9 Best Reverse Engineering Software \[Top Tools for 2020 \] \(apriorit.com\)](#)

Ejemplo

hola.py - C:\Users\marle\Downloads\PC Tema 5\hola.py (3.9.0)

File Edit Format Run Options Window Help

```
print("Hola mundo!")
```

<input type="checkbox"/> Name	Date modified	Type	Size
 hola	11/27/2020 12:07 PM	Application	6,686 KB
 hola	11/27/2020 12:11 PM	IDA (64-bit) Database	4,291 KB
 hola.id0	11/27/2020 12:11 PM	ID0 File	3,432 KB
 hola.id1	11/27/2020 12:08 PM	ID1 File	824 KB
 hola.id2	11/27/2020 12:11 PM	ID2 File	5 KB
 hola.nam	11/27/2020 12:08 PM	NAM File	0 KB
 hola.til	11/27/2020 12:11 PM	TIL File	6 KB

Ejecutable desensamblado

```
;
; +-----+
; | This file has been generated by The Interactive Disassembler (IDA) |
; | Copyright (c) 2018 Hex-Rays, <support@hex-rays.com> |
; | Freeware version |
; +-----+
;
; Input SHA256 : 63598C3D1F37F4E61A34CE88415E50703A3FB6BAE9D59DB4299B804A39C354D0
; Input MD5 : D74F3F0C21CC6A523913BBB183A618A5
; Input CRC32 : 9B5EDFAE
;
; File Name : C:\Users\marle\Downloads\PC Tema 5\dist\hola.exe
; Format : Portable executable for AMD64 (PE)
; Imagebase : 140000000
; Timestamp : 5FB4E0EE (Wed Nov 18 08:53:02 2020)
; Section 1. (virtual address 00001000)
; Virtual size : 00020D60 ( 134496.)
; Section size in file : 00020E00 ( 134656.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment : default
; OS type : MS Windows
; Application type: Executable

include uni.inc ; see unicode subdir of ida for info on unicode

.686p
.mmx
.model flat

; Segment type: Pure code
; Segment permissions: Read/Execute
_text segment para public 'CODE' use64
assume cs:_text
;org 140001000h
```

```

assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing

; int __cdecl main(int argc, const char **argv, const char **envp)
main proc near

arg_0= qword ptr 8

mov     [rsp+arg_0], rbx
push    rdi
sub     rsp, 20h
mov     edi, ecx
call    sub_14000A1A8
mov     rbx, rax
call    sub_14000A1A0
mov     rdx, [rbx]
mov     ecx, [rax]
call    sub_140004F50
mov     rdx, rax
mov     ecx, edi
mov     rbx, [rsp+28h+arg_0]
add     rsp, 20h
pop     rdi
jmp     sub_140002540
main endp

```

Herramientas de Ingeniería Inversa

El proceso de ingeniería inversa implica el uso de ciertas herramientas que consisten en:

- **Desensambladores.** Los desensambladores se utilizan para traducir códigos binarios en códigos de ensamblado (lenguaje ensamblador). También se emplean en la extracción de cadenas, funciones (tanto importadas como exportadas), bibliotecas, etc. Ayudan a convertir el lenguaje de la máquina en un formato más fácil de usar. Diferentes desensambladores se utilizan para diversos propósitos.
- **Depuradores.** Los depuradores contribuyen a ampliar la funcionalidad de los desensambladores mediante la compatibilidad con los registros de CPU, el volcado hexadecimal de programas, la vista de la pila, entre otras cosas. Los programadores utilizan depuradores para establecer puntos de interrupción, así como para editar códigos de ensamblado en tiempo de ejecución. Se utilizan en el análisis de binarios de la misma manera que los desensambladores. Además, permiten recorrer el código ejecutando una línea a la vez para investigar los resultados.
- **Editores hexadecimales.** Los editores hexadecimales permiten a los programadores ver y editar archivos binarios de acuerdo con los requisitos de software. Ayudan a hacer posible manipular los datos binarios fundamentales que componen un archivo de computadora. Por otra parte, debido a que se utilizan para editar archivos binarios, a veces se conocen como un editor binario o un editor de archivos binarios.
- **Explorador de Programas y visor de recursos.** Herramientas que permiten a los programadores ver y editar los recursos incrustados en el archivo EXE. Les permiten cambiar iconos, editar menú, información de la versión, diálogo, etc. Un ejemplo es PE Explorer, que facilita la traducción de aplicaciones que no tienen códigos fuente.

Ingeniería Inversa de Software en Ciberseguridad

Los principales uso de la ingeniería inversa de software en Ciberseguridad son:

- Analizar cuan difícil es hackear un software específico, para de esta forma generar recomendaciones de como "complicar" el trabajo para los hackers potenciales.
- Proteger datos en entornos tales como el cómputo en la nube, gracias a que se aplica la ingeniería inversa para encontrar vulnerabilidades en software antes de que salga a producción, permitiendo mejorar la seguridad y agregar capas de protección.
- Este tipo de acciones también ayuda a combatir exploits de día cero (zero-day exploits).

Referencias

- https://link.springer.com/chapter/10.1007/978-3-642-04117-4_31
- https://es.wikipedia.org/wiki/Ingenier%C3%ADa_inversa

- <https://securitytoday.com/articles/2019/02/26/reverse-engineering-is-one-of-your-best-weapons-in-the-fight-against-cyberattacks.aspx>
- <https://resources.infosecinstitute.com/topic/hacking-tools-reverse-engineering/>