Reverse Engineering II

CC5325 - Taller de Hacking Competitivo
Diego Vargas

Contenidos

- Obfuscación
- Técnicas de Deobfuscación
- Demo

Obfuscación

Definición

Wikipedia:

> La ofuscación se refiere a encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar.
>
> En computación, la ofuscación se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático, en el código intermedio (bytecodes) o en el código máquina cuando el programa está en forma compilada o binaria.

Objetivo

El objetivo principal de la obfuscación es dificultar la comprensión del código. Esto no evita que alguien con suficiente tiempo, motivación y conocimiento pueda llegar a entender el código, pero sí impone un trabajo adicional y previo al análisis normal.

Nosotros solo veremos obfuscación de código fuente, no veremos obfuscación de código compilado.

Técnicas de Obfuscación

- **Renaming**: Cambiar nombres y referencias.
- **Eval**: Evaluar un string codificado.
- **String splitting**: Separar strings en muchas variables.
- **Dead branches**: Caminos condicionales que nunca se ejecutan.

En la práctica se aplica una combinación de estas técnicas en diferentes partes del código para dificultar aún más el proceso de reversing.

Técnicas de Deobfuscación

Evaluación Manual

Se revisa el código manualmente, renombrando variables, funciones y clases, decodificando strings y otras constantes, quitando ramas condicionales que no se ejecutan, etc.

Se suele ejecutar línea por línea, estilo debugger, para revisar el valor de los diferentes objetos y variables en tiempo de ejecución.

Se puede aplicar a códigos pequeños y de poca complejidad, ya que usualmente toma bastante tiempo y dedicación.

Uso de Herramientas Automatizadas

Existen muchas herramientas automatizadas que se encargan de deobfuscar el código y retornar algo más legible. Suelen ser muy fáciles de usar y, dependiendo del caso, pueden funcionar muy efectivamente.

Sin embargo, no siempre funcionan, por lo que se debe buscar otras herramientas o realizar deobfuscación manual.

Evaluación Mixta

Esta es la técnica que comúnmente se utiliza en el mundo real. Se combina la evaluación manual con el uso de herramientas para maximizar la legibilidad y comprensión del código final.

Primero se debe identificar el lenguaje y técnicas de obfuscación utilizadas. Luego, iterativamente se pasa el código por herramientas de deobfuscación, se analiza el resultado y se realiza cambios manuales.

El resultado debería ser más legible que usando cada una de las técnicas por separado.

Demo

Demo

- Varios problemas de HTB/TryHackMe.