INTRODUCCIÓN AL REVERSING

CON IDA PRO DESDE CERO PARTE

29

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Con lo que hemos visto hasta ahora podemos intentar al menos analizar programas reales, para ellos les daré un ejercicio que en la parte 30 solucionare yo, me gustaría que lo tomen como algo divertido y que me envíen lo que encuentren.

Aclaro que no es nada fácil, así que no se depriman jeje.

La idea es que les doy dos versiones consecutivas de un programa, así que puede haber en la más nueva parches que se pueden hallar diffeando o analizando.

Yo les aconsejo hacer un diff como vimos en las partes anteriores y tratar de ver si hay overflows y me lo envían no es necesario escribir código solo hallar funciones vulnerables en el que quieran.

Adjuntos están los instaladores en su versión más vieja y nueva, quizás lo mejor sería en una máquina virtual instalar el viejo hacer un snapshot y luego el nuevo y otro, así se pueden extraer los archivos para diffear de ambas.

La idea es divertirse y jugar un rato no importa si les sale o no esta bueno intentar.

Cómo ayuda pueden ver el CVE.

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4654>

La vulnerabilidad es al abrir un archivo de extensión .ty en VLC hasta 0.94 inclusive.

Hasta la parte 30.

Ricardo Narvaja