Instituto Tecnológico de San Juan del Río

Tópicos de ciberseguridad

P R E S E N T A:

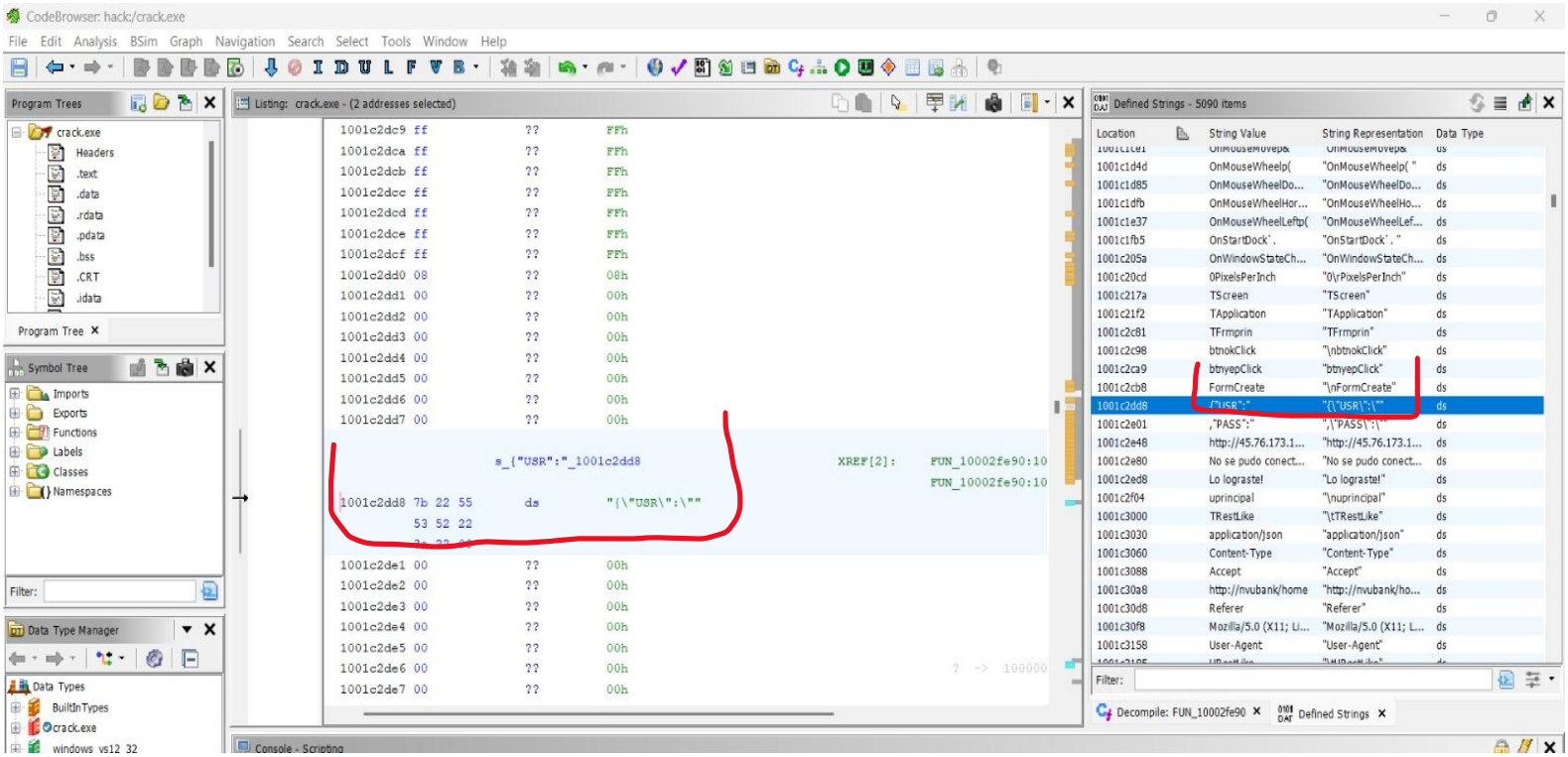
Abelardo Garduño Fuertes 22590040
Alejandro Pérez Piña 22590068
Brandon Ismael Trejo Hernández 22590049

Ingeniería en Sistemas Computacionales

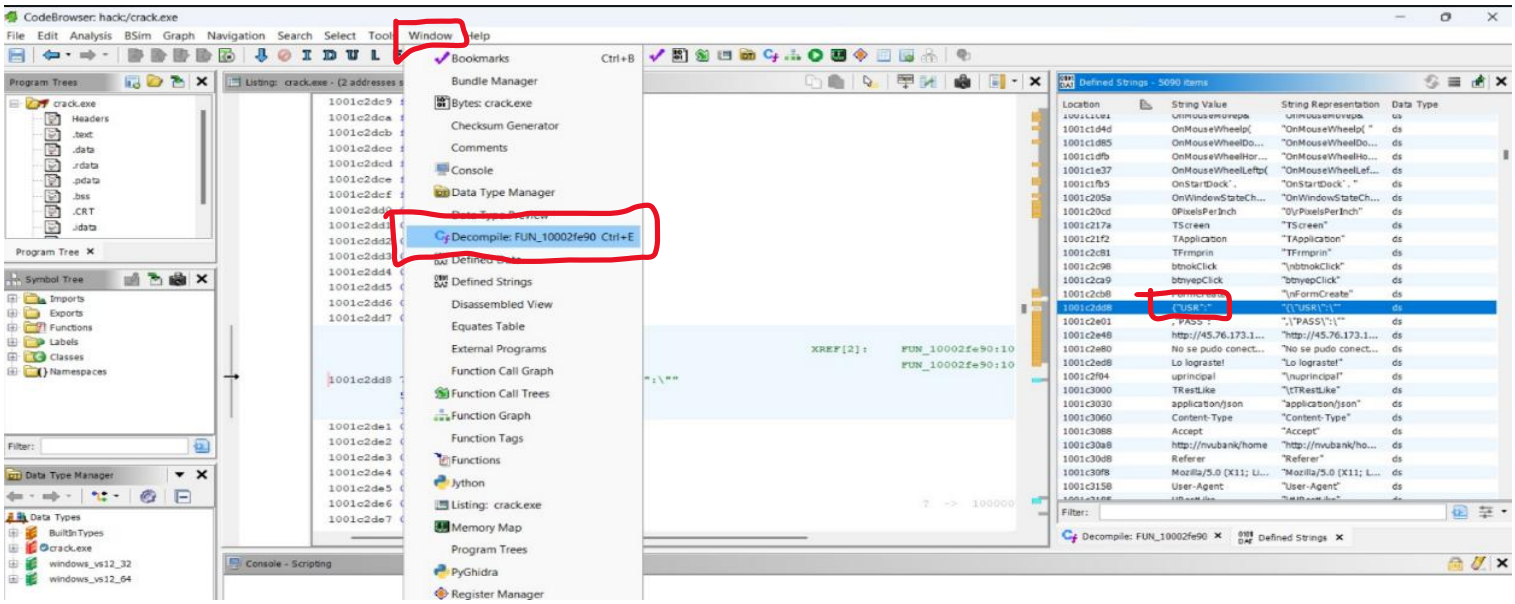
PERIODO [ENE-JUN 2026]

ENLACE AL VIDEO - https://youtu.be/c3V1gDUp9kc

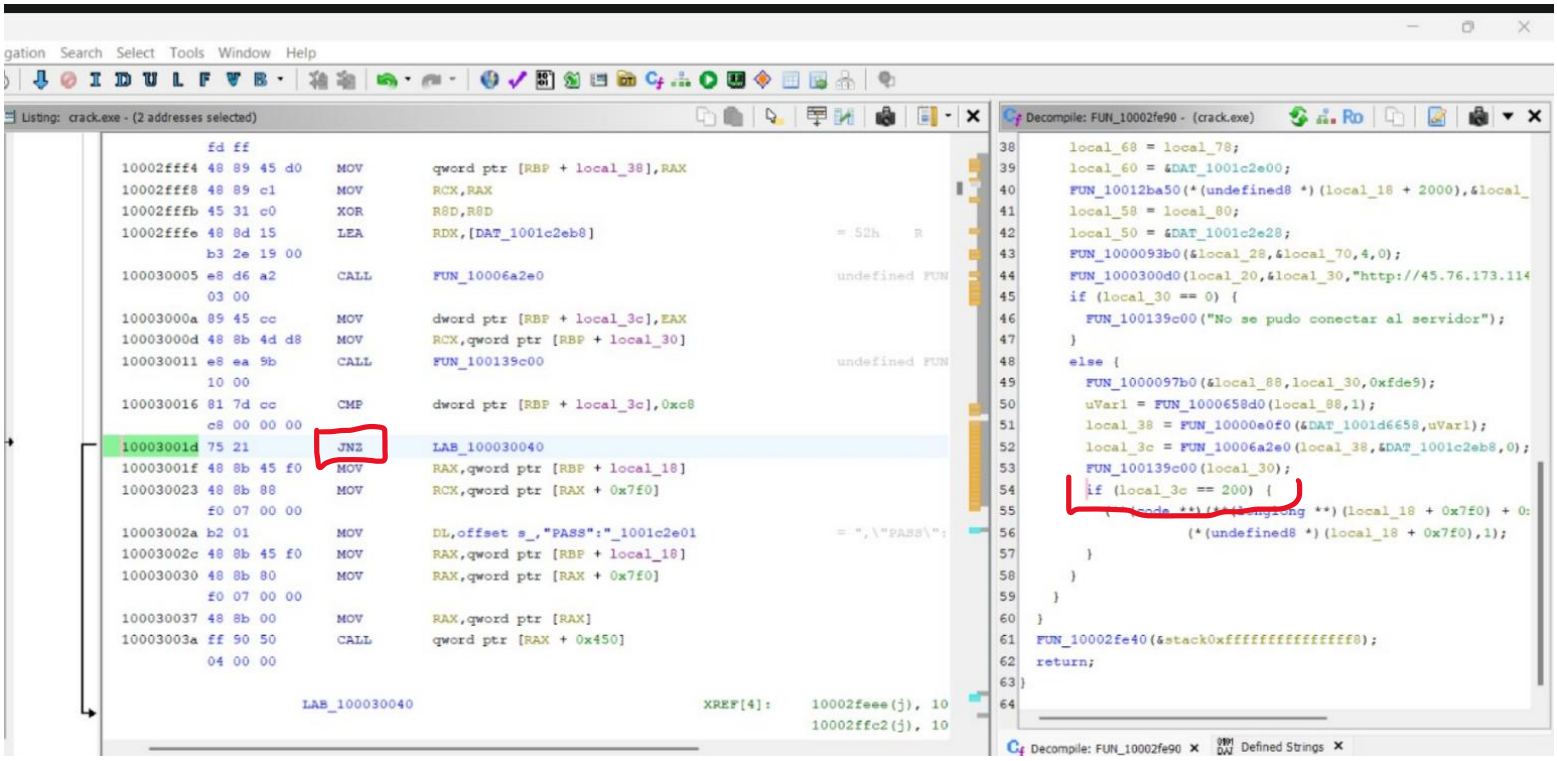
Abrimos el ejecutable con ghidra y ocupamos la opción define strings y observamos que aparecen las variables donde se define el usuario y contraseña en la base de datos (“USR” y “PWD”).



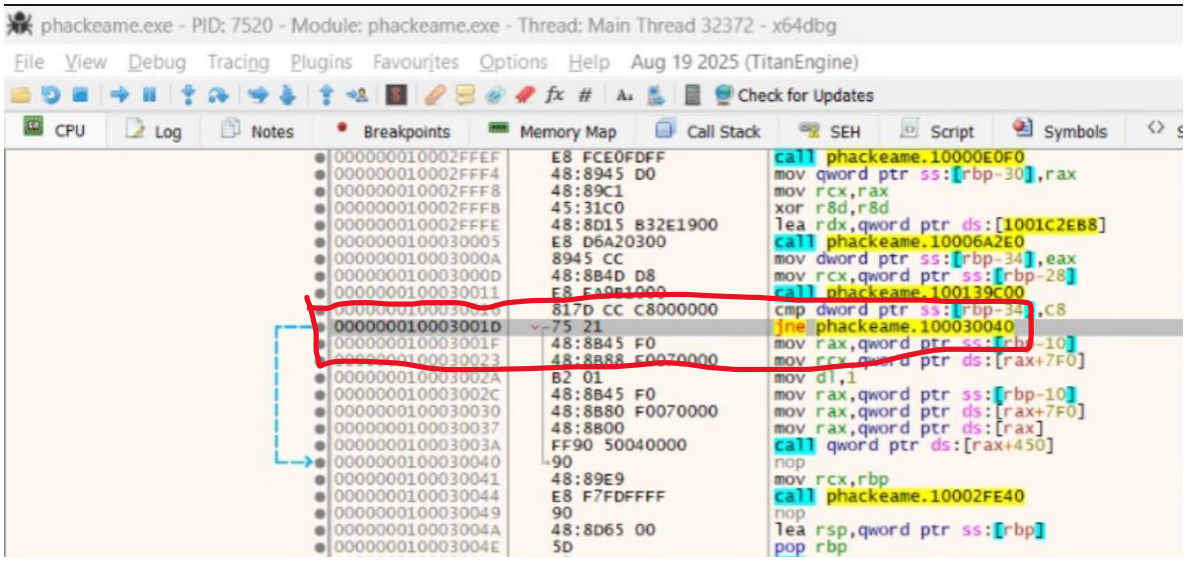
En el apartado Window (Parte superior de la pantalla), seleccionamos la opción “Decompile” mientras seleccionamos la variable “USR” en el apartado define strings.



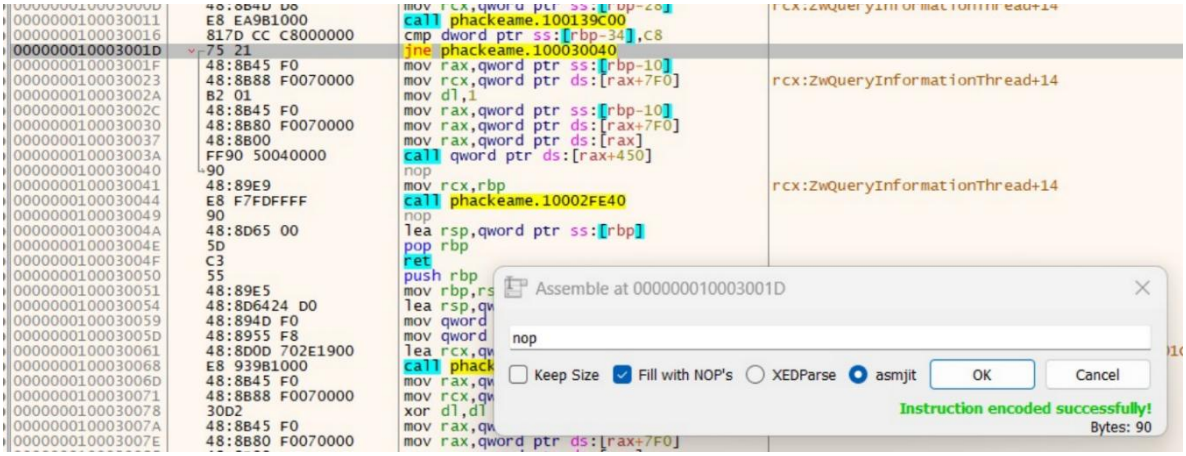
Una vez seleccionada esa opción, podemos ver el código, en donde, si prestamos atención, podemos ver que hay una parte en donde podemos ver una validación donde nos dice que no se pudo conectar al servidor. Siguiendo la lógica del código vista en clase, la siguiente validación es la que creemos que hace que valide el usuario accedido. Si damos click a ese if, podemos ver que en la parte de la izquierda hace un salto si es diferente de cero.

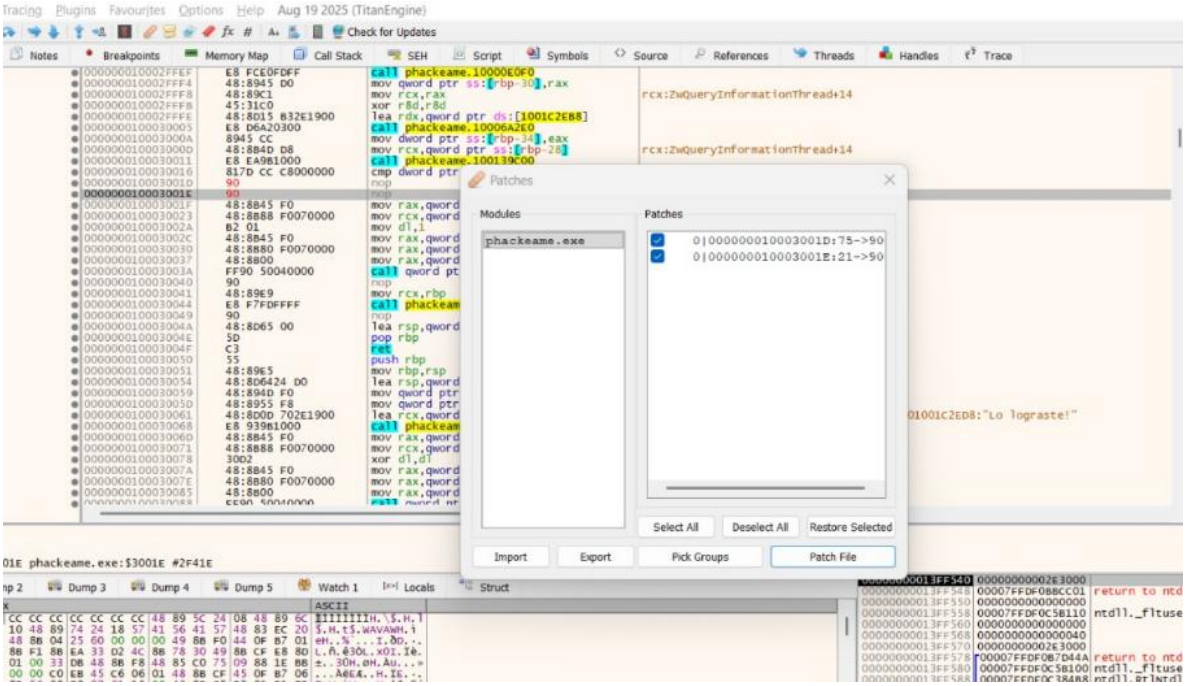


Si observamos, se resalta la posición de memoria en donde se encuentra ese salto. Conociendo la información, en el debug x64 buscamos esa posición de memoria a través del step over y step into, encontrando el salto.



Desensamblamos el salto con click derecho y le ponemos nop y la parchamos.





Y finalmente, conseguimos hackear la app.