Instituto Tecnológico de San Juan del Río

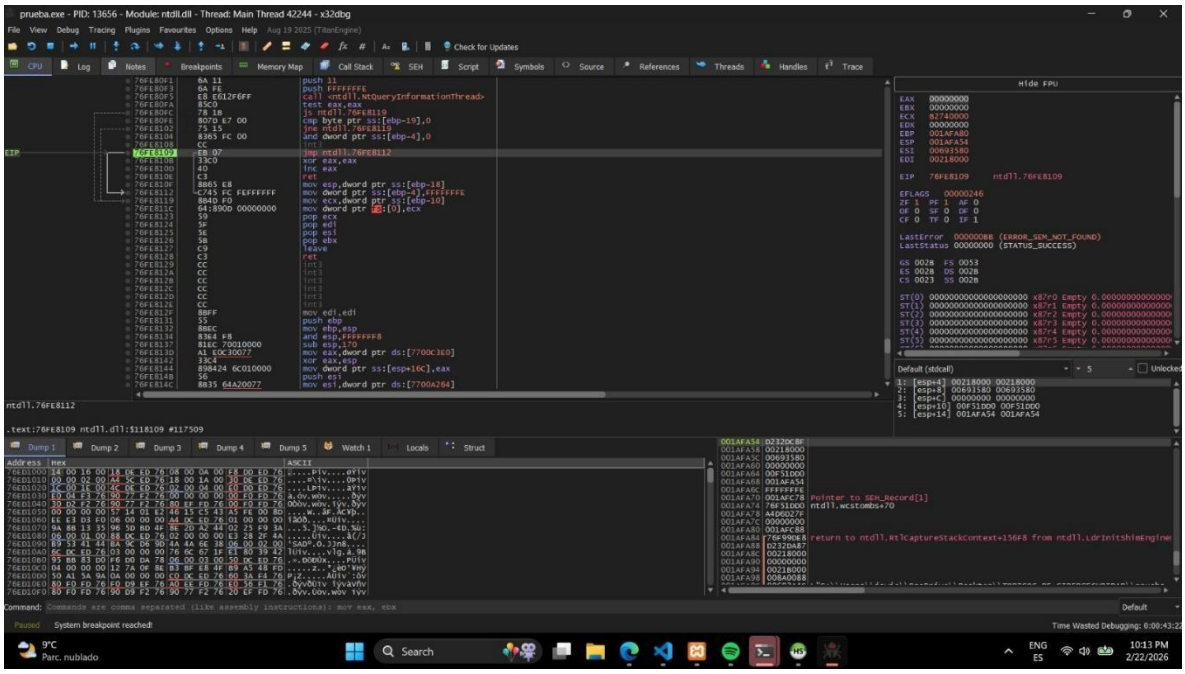
Tópicos de ciberseguridad

P R E S E N T A:

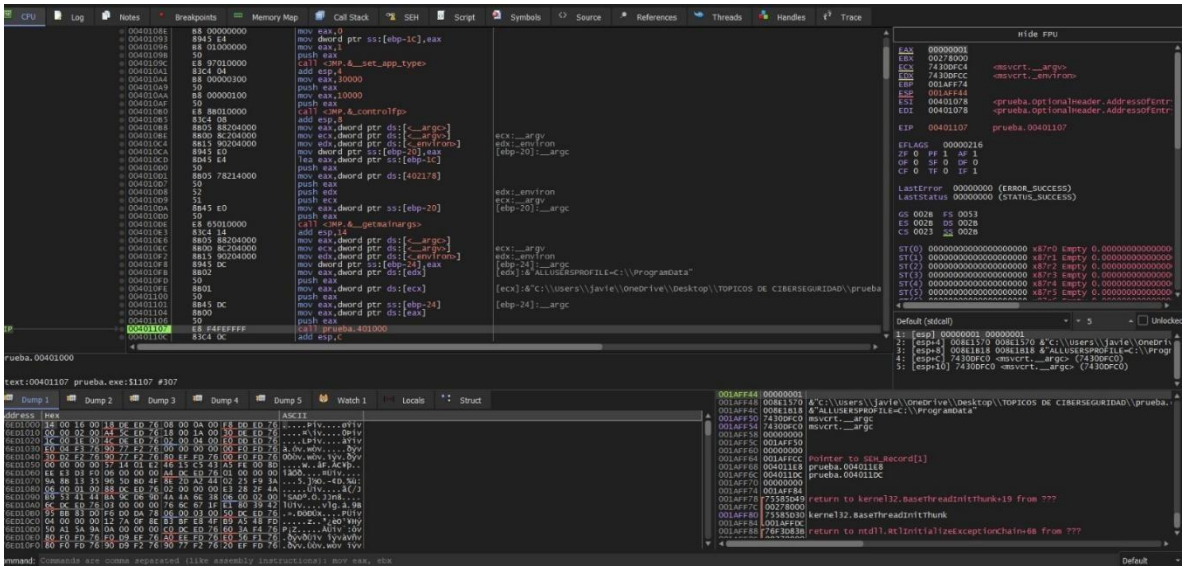
Pablo Colunga Ochoa
Andres Martin Sinecio
Javier Hernandez Mendoza

Ingeniería en Sistemas Computacionales

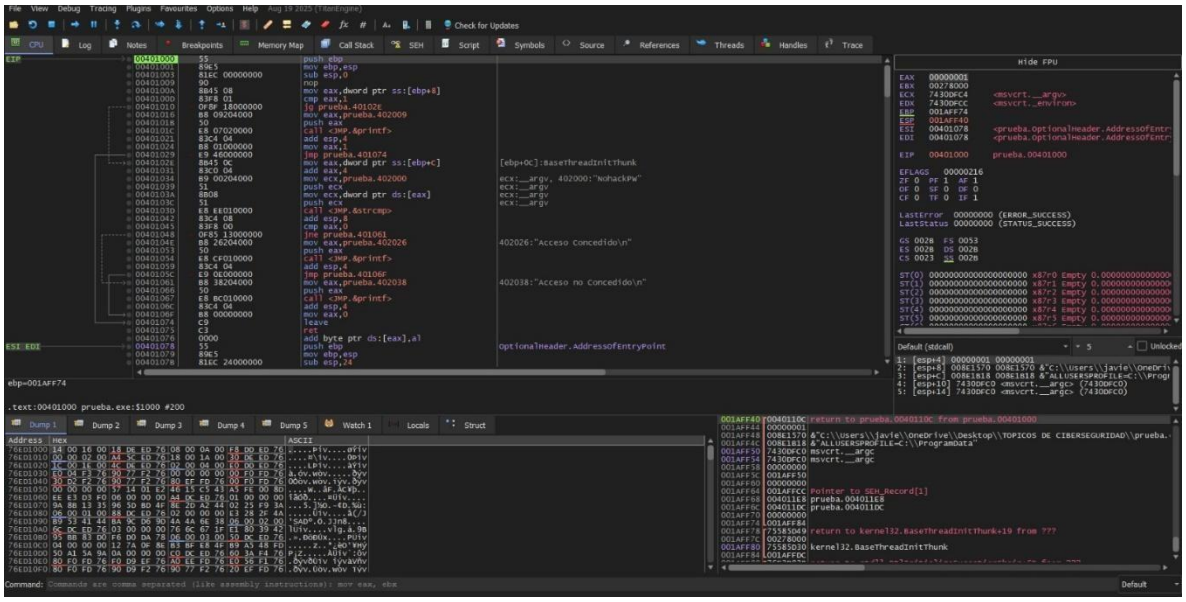
PERIODO [ENE-JUN 2026]



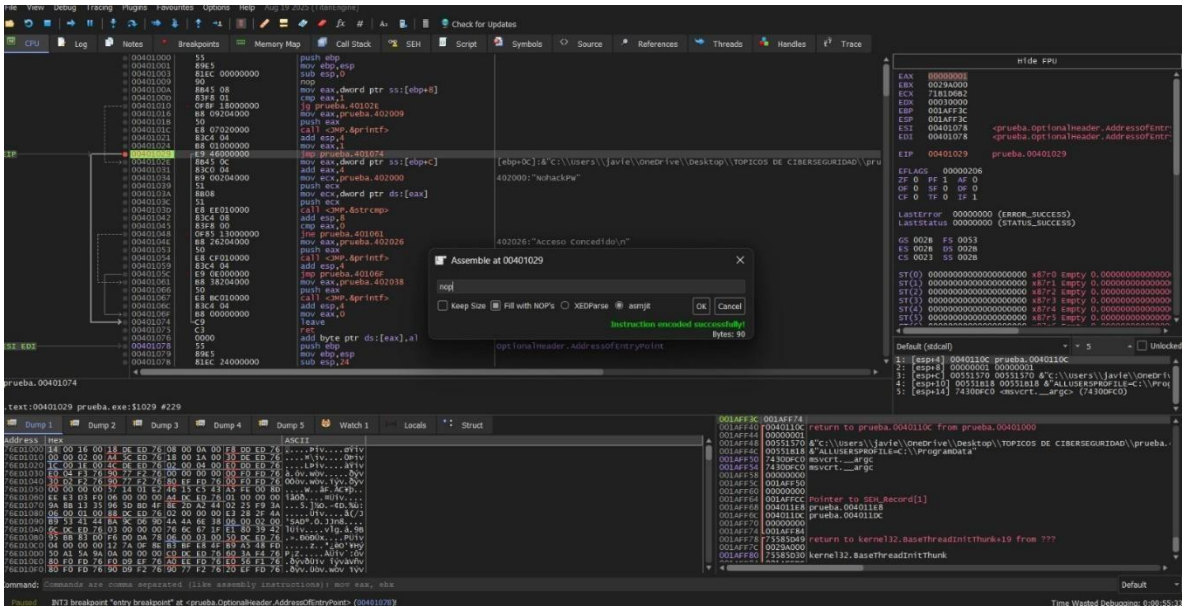
cargamos el archivo "prueba" dentro del debugerx32



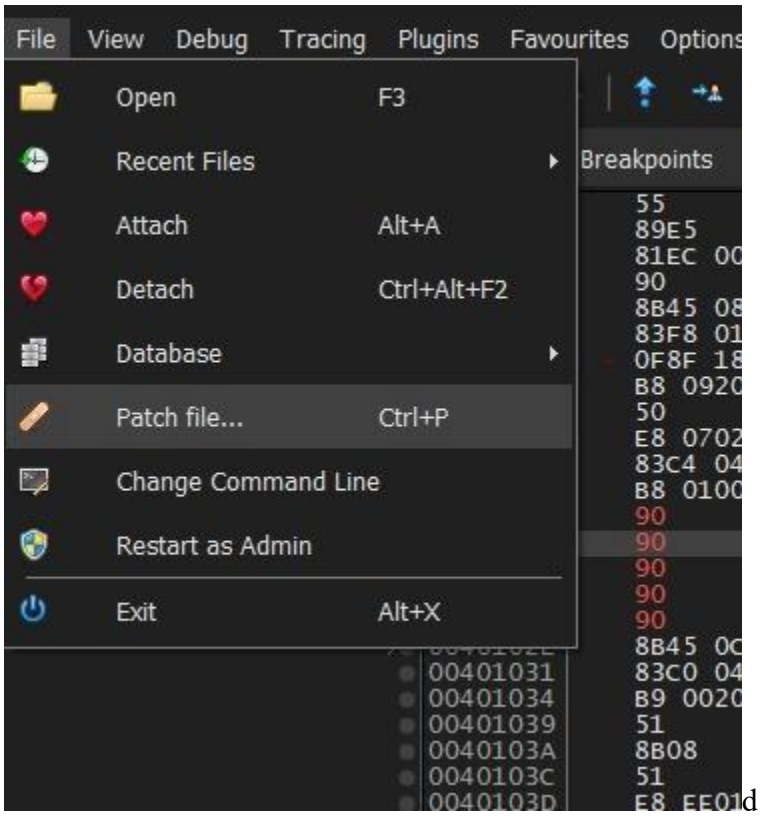
Identifiqué el main porque después de __getmainargs (que construye argc/argv), el runtime hace call prueba.00401000, y al hacer Step Into se entra al código propio del ejecutable, que corresponde al inicio de la lógica principal.



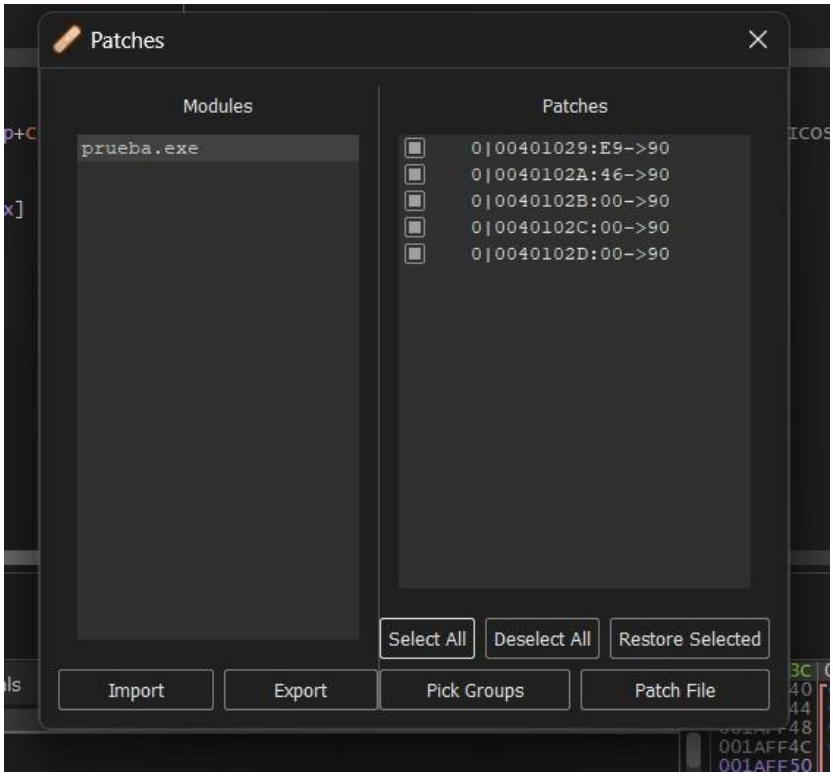
Después de la inicialización del runtime (MSVCRT), al ejecutar Step Into sobre call prueba.00401000, el flujo entra a prueba.exe en la dirección 00401000. En esta función ya se observa lógica propia del programa: lectura de argumentos (argv), comparación de cadenas y mensajes de salida, lo que indica que corresponde al inicio de la rutina principal (main lógico).



Se identificó una instrucción de transferencia de control (salto) en el flujo principal de ejecución y se sustituyó por instrucciones NOP, eliminando la redirección y forzando la continuidad secuencial del código. La modificación se realizó mediante re-ensamblado en x32dbg, quedando registrada en la dirección virtual correspondiente y reflejada en el byte de operación 0x90, como evidencia del parche aplicado.



Se parcheó el archivo



```
PS C:\Users\javie\OneDrive\Desktop\TOPICOS DE CIBERSEGURIDAD> .\pruebapycrack.exe hola
Acceso Concedido
PS C:\Users\javie\OneDrive\Desktop\TOPICOS DE CIBERSEGURIDAD>
```

corrimos el programa con cualquier contraseña dandonos el acceso

```
PS C:\Users\javie\OneDrive\Desktop\TOPICOS DE CIBERSEGURIDAD> python .\pycrack.py
Bytes a modificar: 0f8513000000
Su parche fue aplicado correctamente> C:\Users\javie\OneDrive\Desktop\TOPICOS DE CIBERSEGURIDAD\pruebaa.exe
PS C:\Users\javie\OneDrive\Desktop\TOPICOS DE CIBERSEGURIDAD>
```

se utilizo el python para hacer la modificacion de los bytes correspondientes y se aplica el parche en un archivo distinto al original