Grado en Ingeniería Informática

Seguridad en Tecnologías de la Información
Curso 2017/18

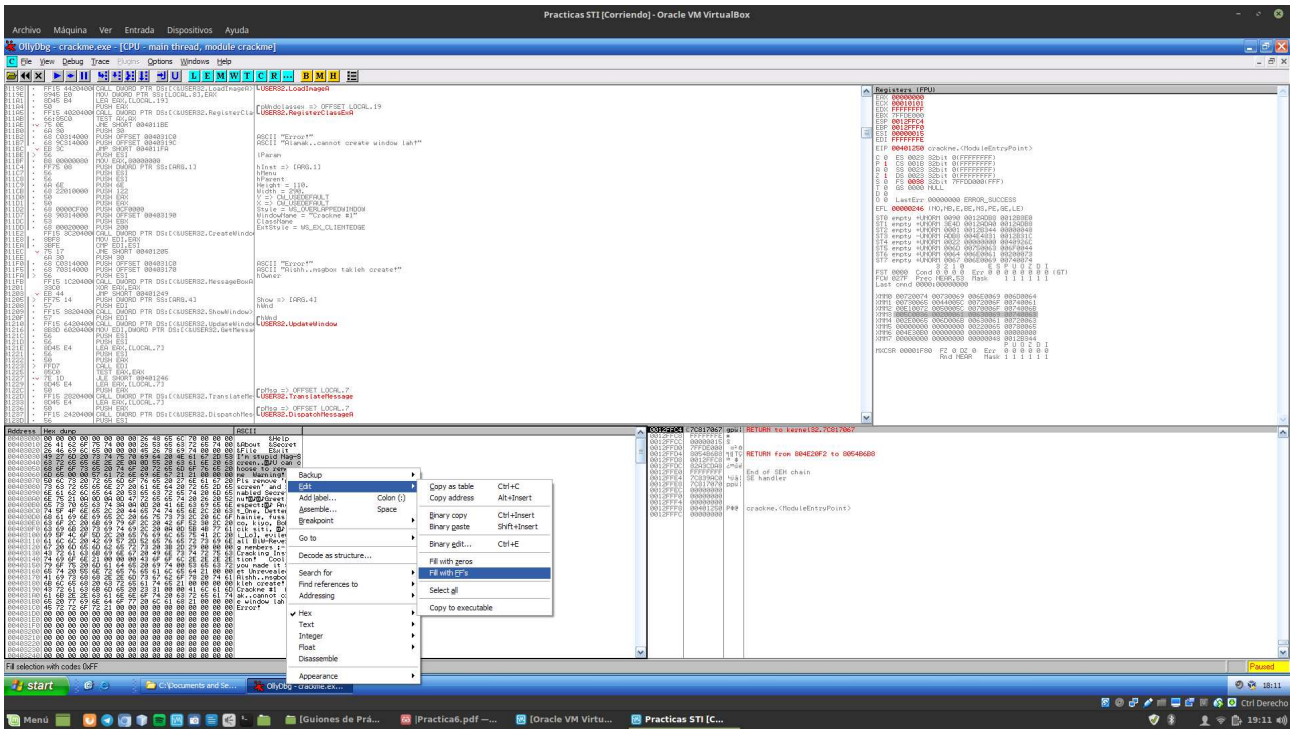
Práctica Número 6

UNIVERSIDAD DE JAÉN

Autor: Manuel Alférez Ruiz

Ventana inicial

En la primera parte nos pedían que modificásemos el programa *crackme.exe* para que no saliese la ventana inicial.



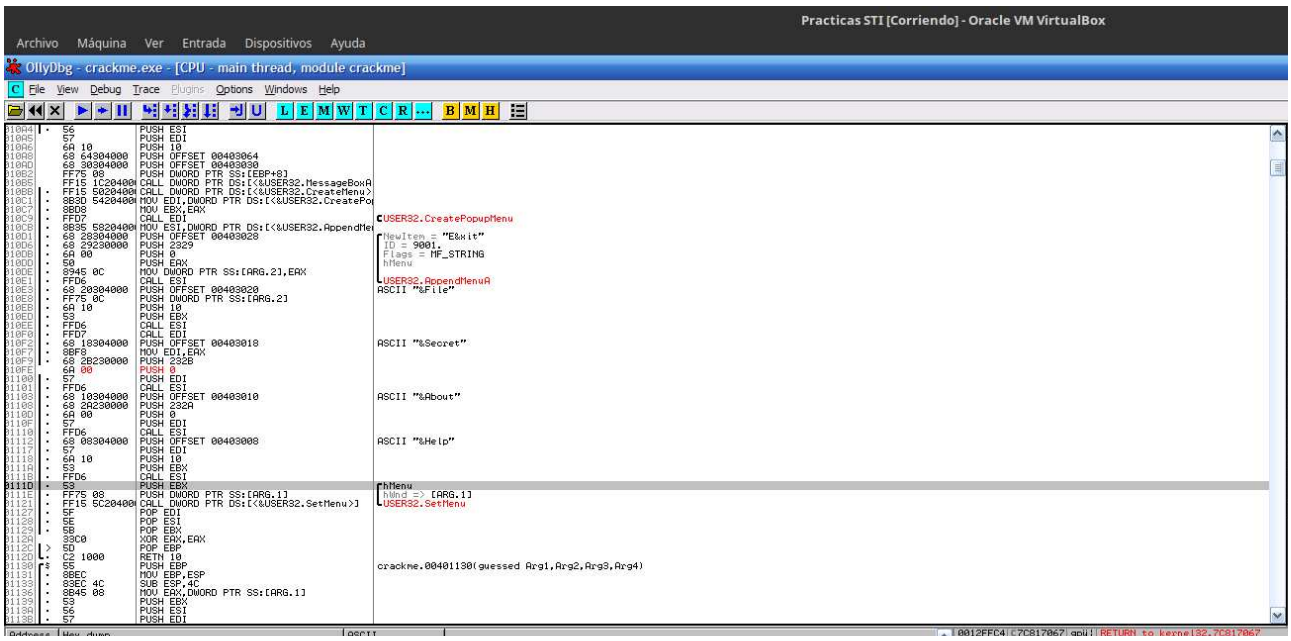
En la esquina inferior izquierda nos aparece un código *ASCII* con el texto del mensaje. Si seguimos estos pasos:

- Seleccionamos el texto
- Clic derecho
- Edit
- Fill with FF's (con lo que nos aparecerán todos los *hex dump*, que tienen una asignación con el texto del mensaje, puestos a FF)

Habremos conseguido que no nos aparezca la ventana inicial, y nos saltaría automáticamente al menú *Crackme #1*.

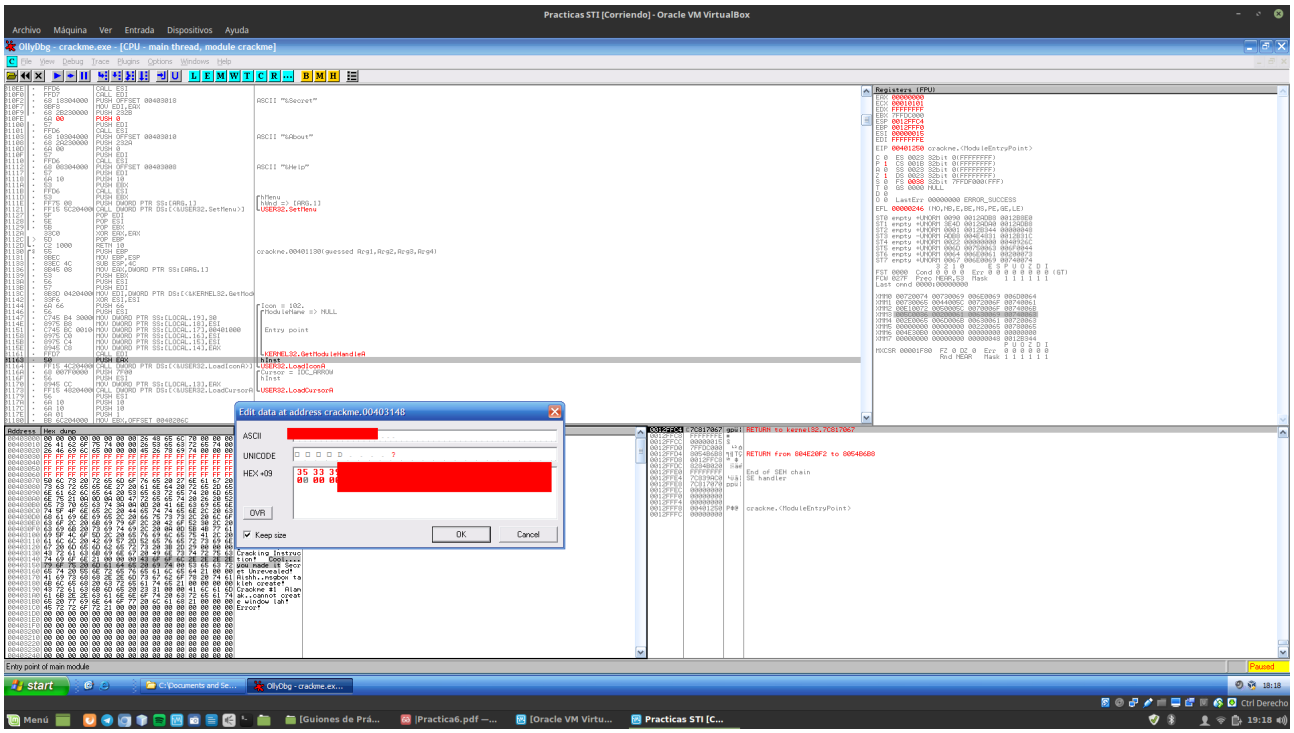
Opción Secret

En esta segunda parte, se explicará los pasos a seguir para habilitar la opción del botón *Secret*.

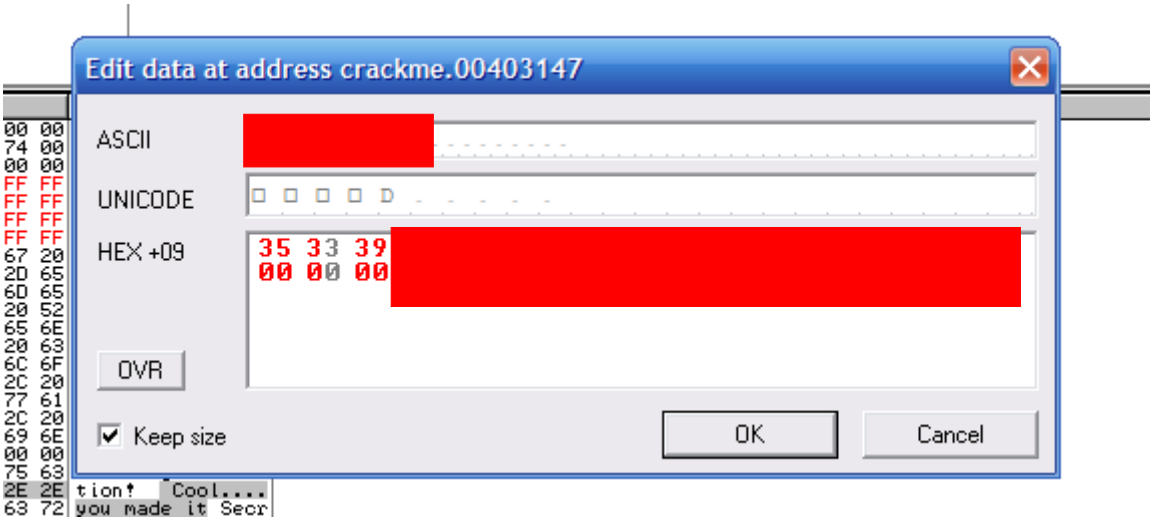


En primer lugar he modificado el *PUSH*, que estaba puesto a 1 (aparece en rojo). Habría que ponerlo a 0 al igual que en *About* para que estuviese también habilitado. Por lo tanto, con este paso ya tendríamos la posibilidad de hacer click sobre el botón *Secret*.

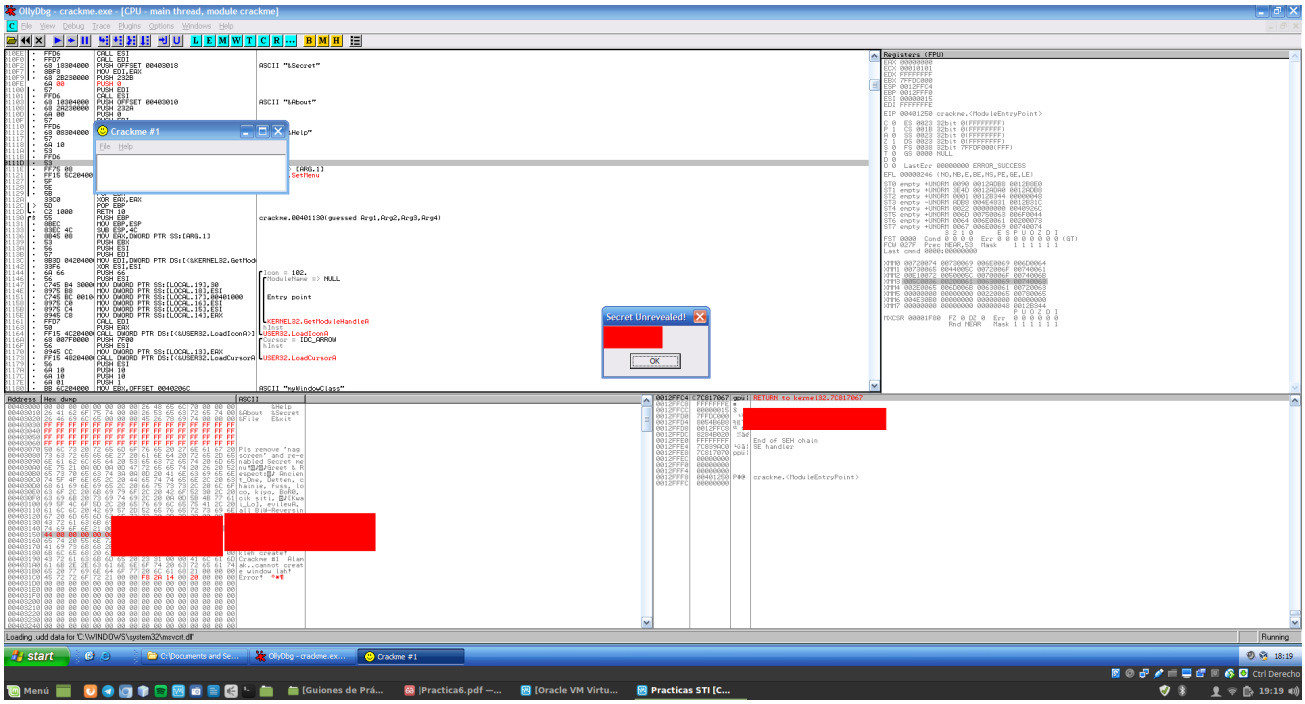
Finalmente, para modificar el mensaje que nos aparece al pulsar el botón *Secret*, bastaría con irnos a la misma zona donde habíamos deshabilitado la ventana emergente.



Por tanto, una vez seleccionado el mensaje que nos aparecía, *“Cool… you made it”*, pulsando Ctrl+E nos aparecerá esta ventana:



Pulsando sobre *HEX+09* ponemos todos a cero y después escribimos en el *ASCII* el mensaje que queremos que se muestre, que para esta práctica es mi DNI: 53911043D



Como podemos ver, ha aparecido el mensaje mostrando el DNI.

Y ha así ha sido la manera en la que he ido procediendo hasta conseguir los dos objetivos de esta práctica.