Instituto Tecnológico de Costa Rica

IC8071 – Seguridad del Software

Profesor: Dr. Herson Esquivel Vargas.

Tarea 5 – Shellcode 1

Estudiante:

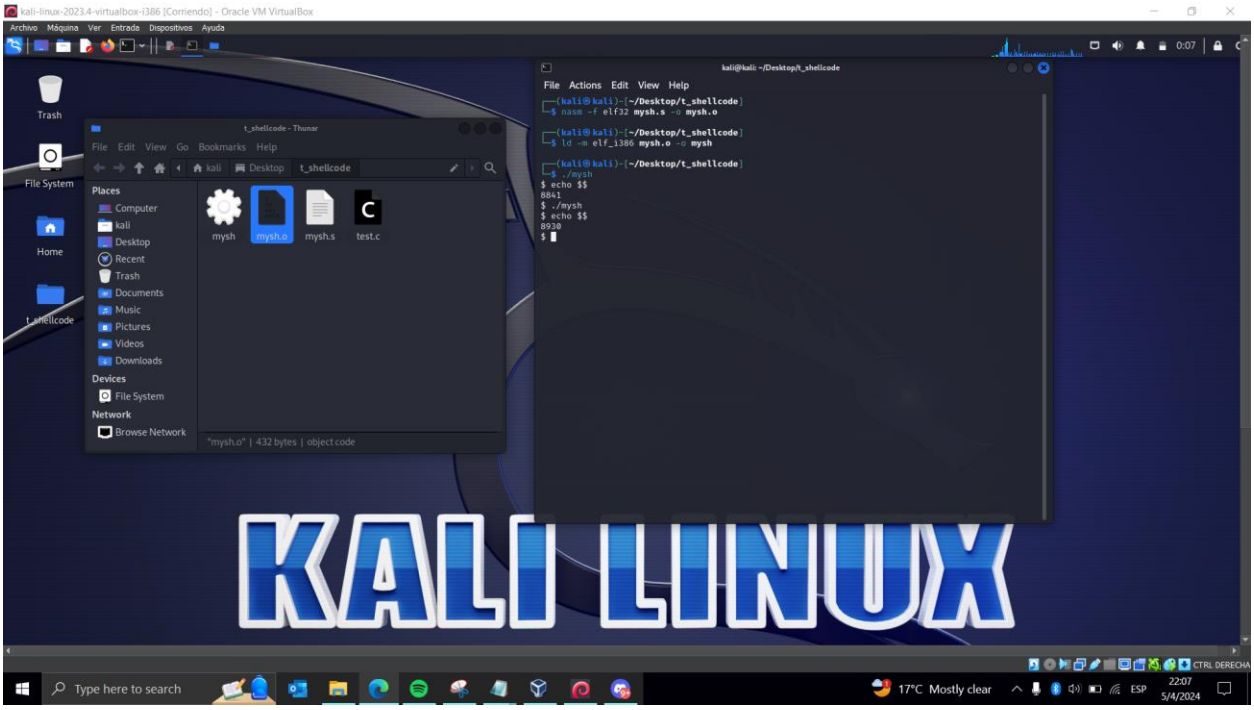
Jose Pablo Hidalgo Navarro – Carné: 2020178017

Axel Alexander Chaves Reyes – Carné: 2021099588

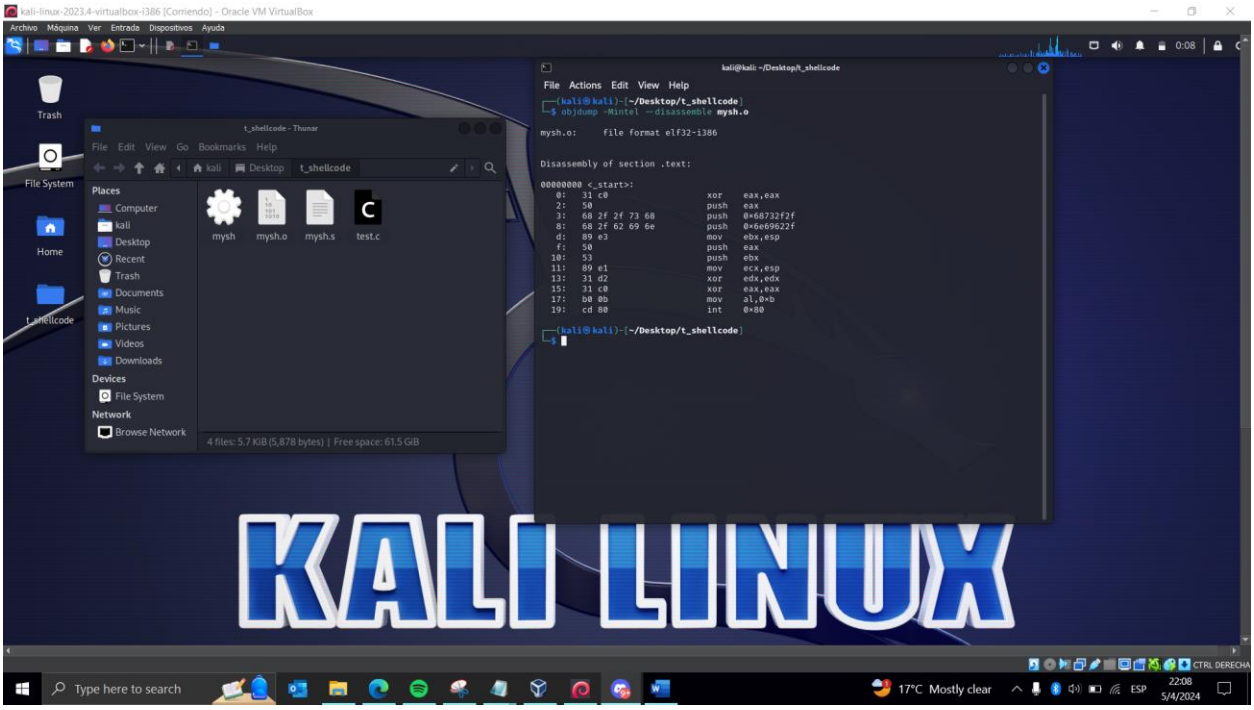
Fecha de entrega: 05/04/2024

I Semestre, 2024

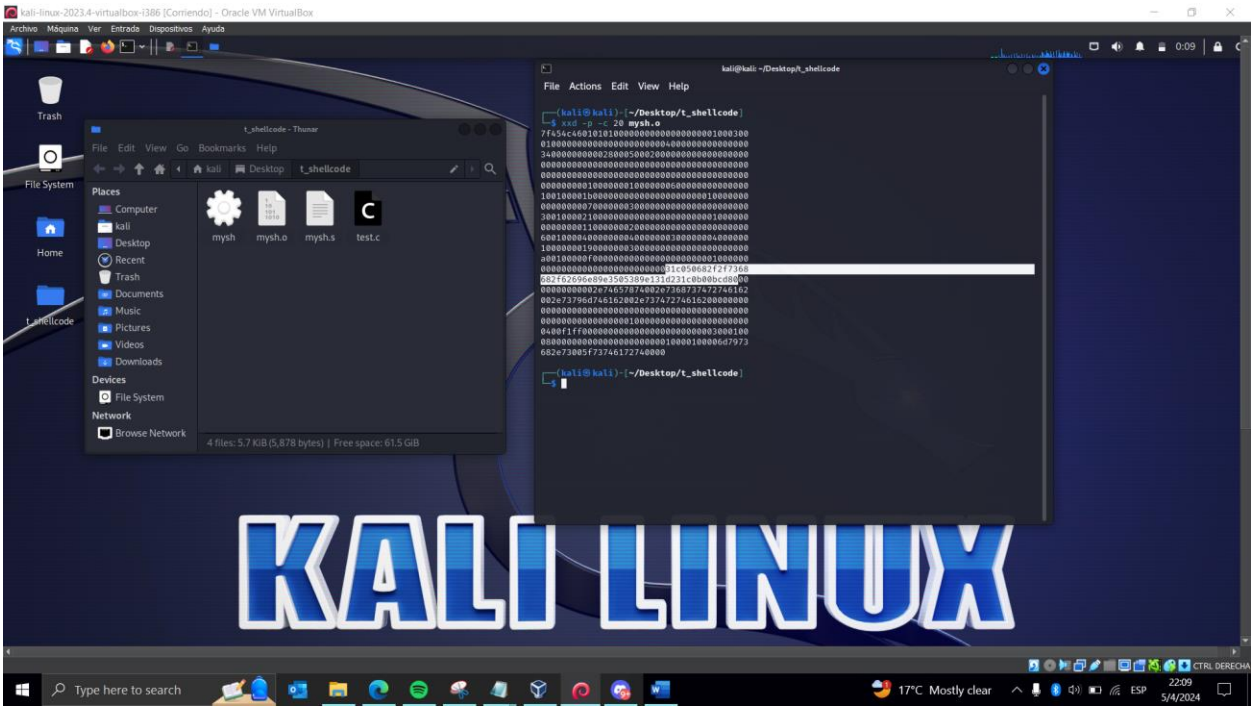
Creación del archivo mysh.s, su -o y su binario. Se ejecutó el binario.



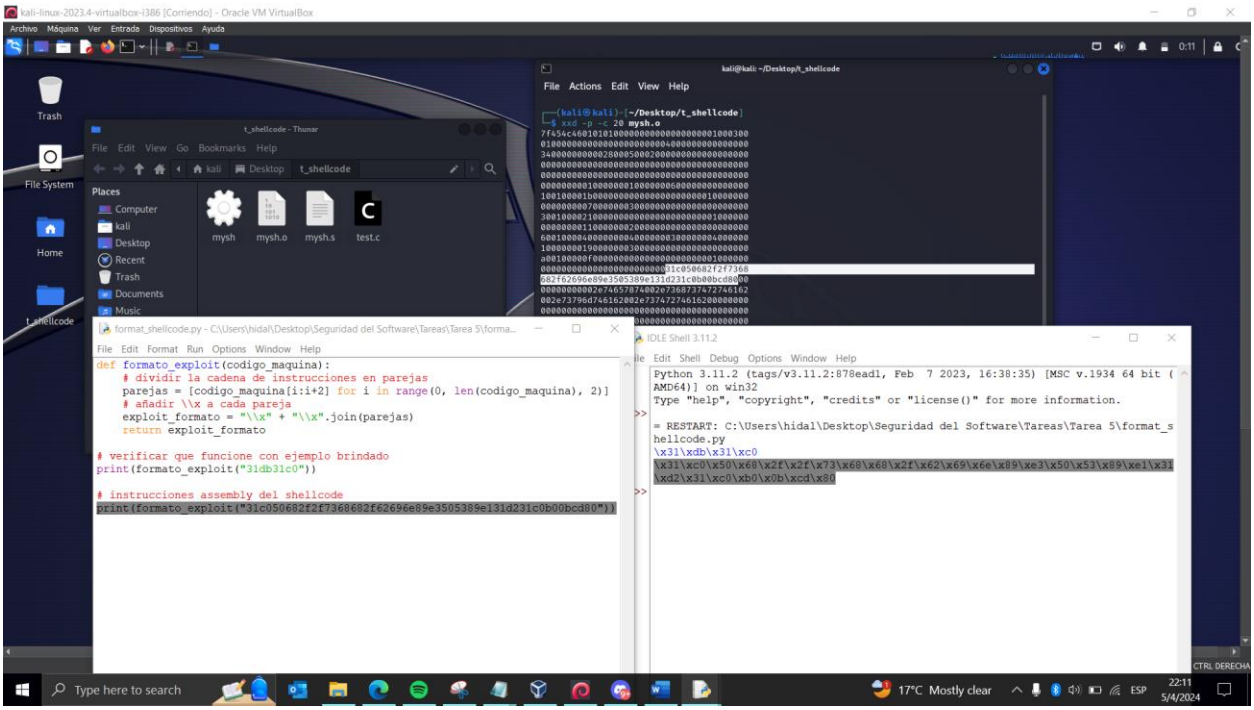
ObjectDump del binario para ver las instrucciones en assembly.



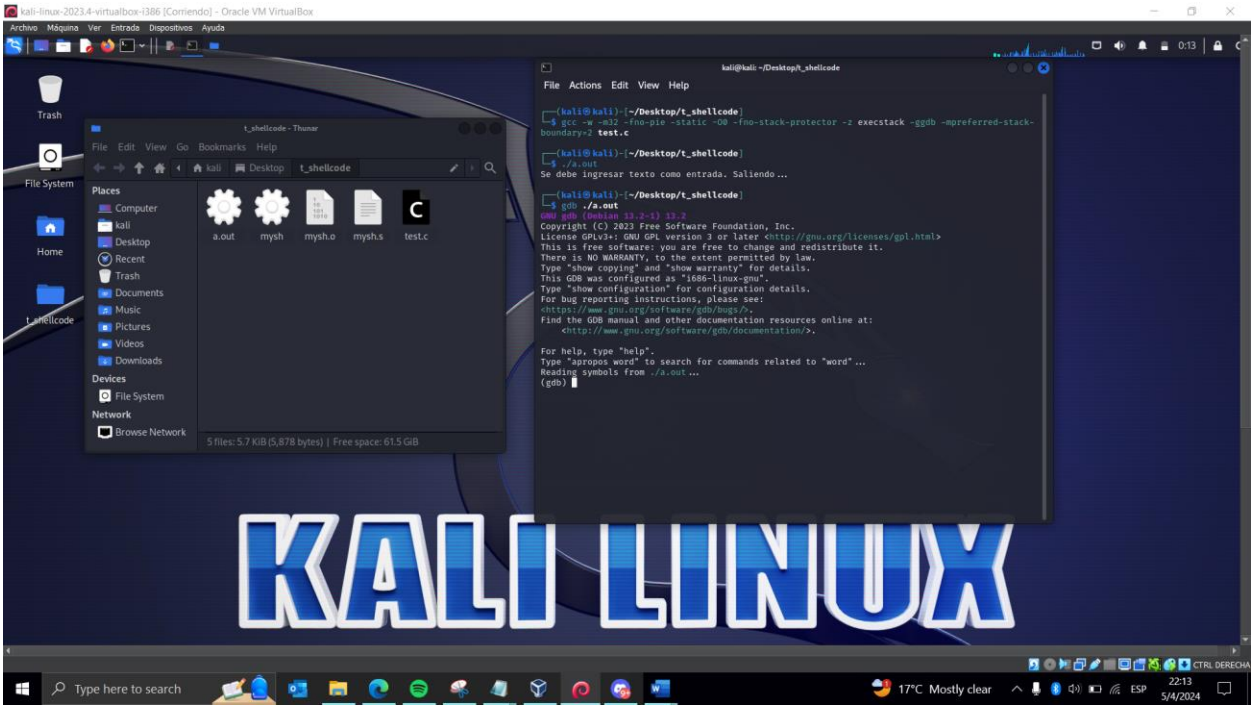
Visualización de las mismas instrucciones con xxd, para eliminar el ruido. Se copiaron las instrucciones para utilizarlas en el script de Python para darles el formato para shellcode.



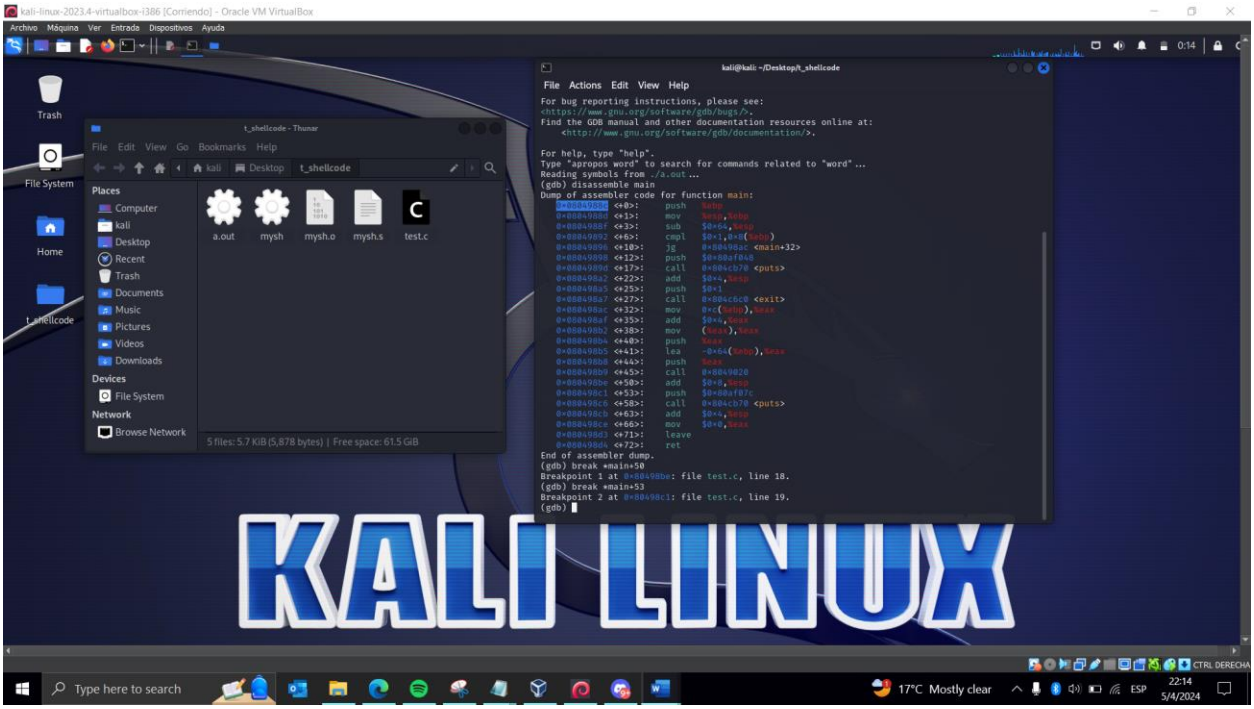
Código de formateo en Python, con la prueba brindada de ejemplo y el set de instrucciones obtenidos en el paso anterior.



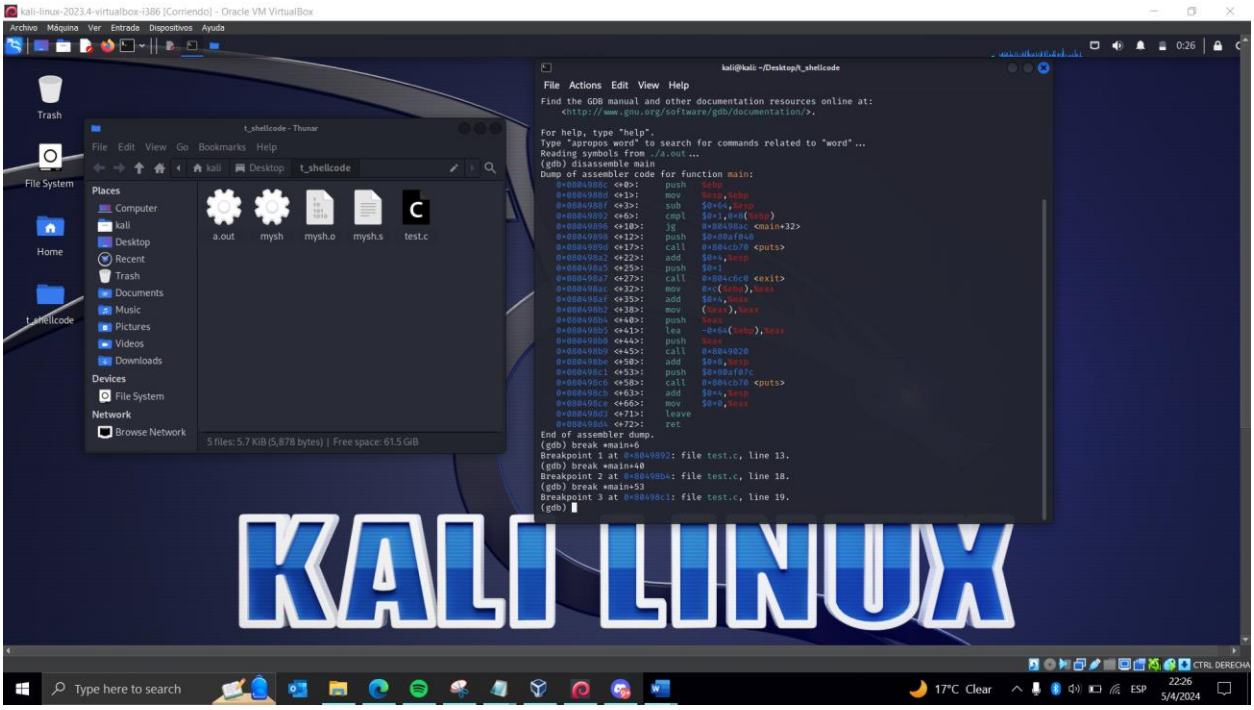
Compilación del test.c (código visto en clase susceptible a shellcode), implementando diversas options para bajar las defensas del programa de compilación. El ejecutable obtenido fue ejecutado y abierto con gdb.



Disassembly de las instrucciones del ejecutable proveniente del test.c



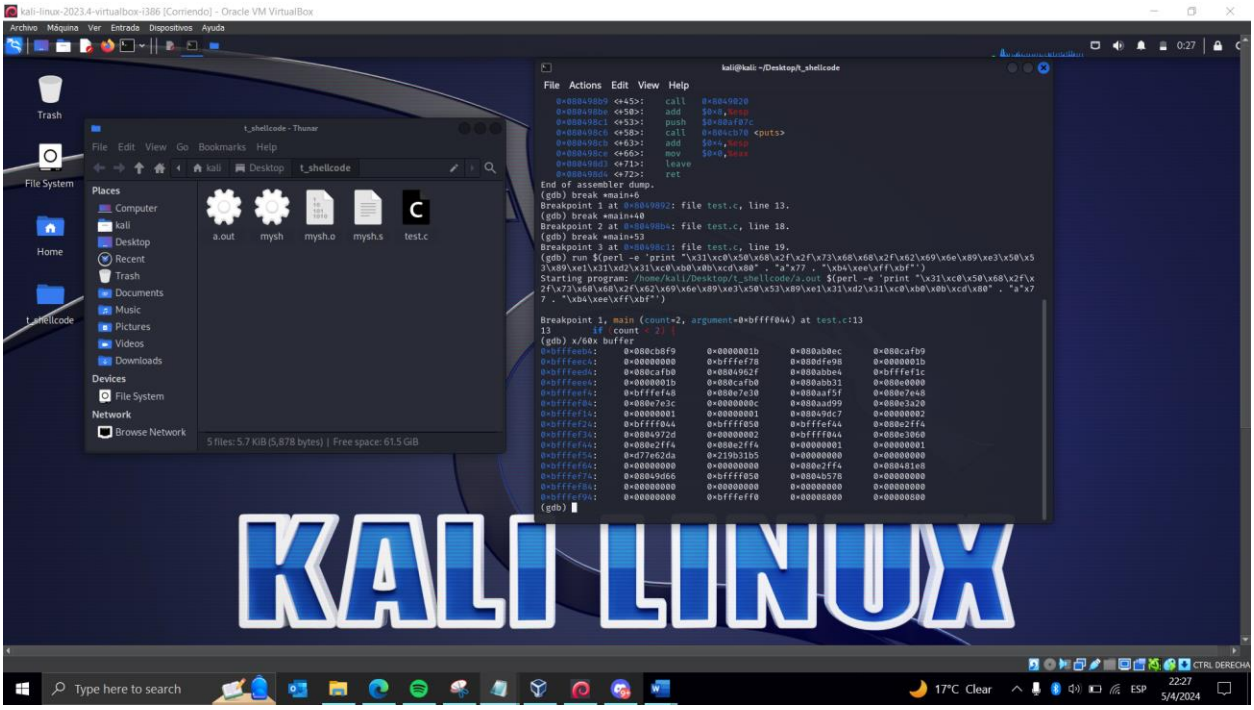
Declaración de 3 breakpoints para revisar el estado del buffer durante el análisis con gbd.



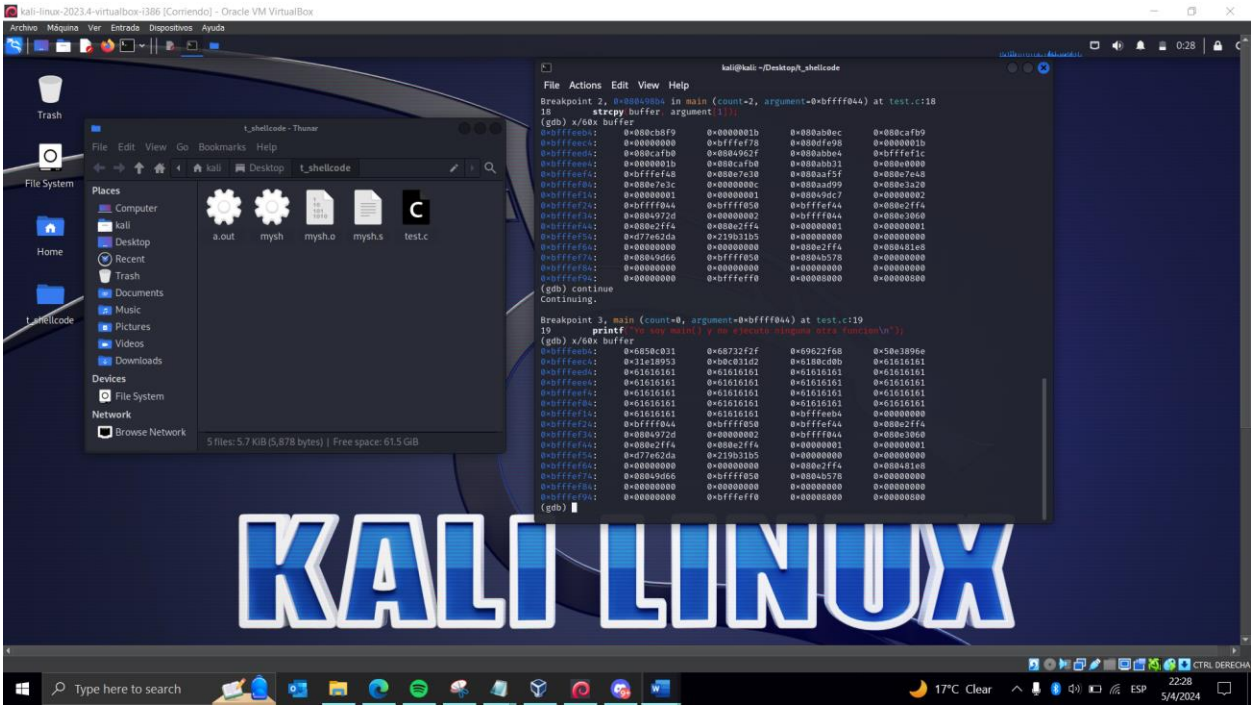
Payload desarrollado: run $(perl -e 'print "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\x31\xc0\xb0\x0b\xcd\x80" . "a"x77 . "\xb4\xee\xff\xbf"')

Se implementó perl para enviar el parámetro tipo String. El orden de este es 1) instrucciones de mysh, 2) 77 “a” para llenar y agotar la memoria del búfer hasta dejar el espacio del return address y 3) la nueva dirección del return address, la cual modificará el stack pointer para que se ejecuten las instrucciones inyectadas al finalizar la ejecución del binario de test.c

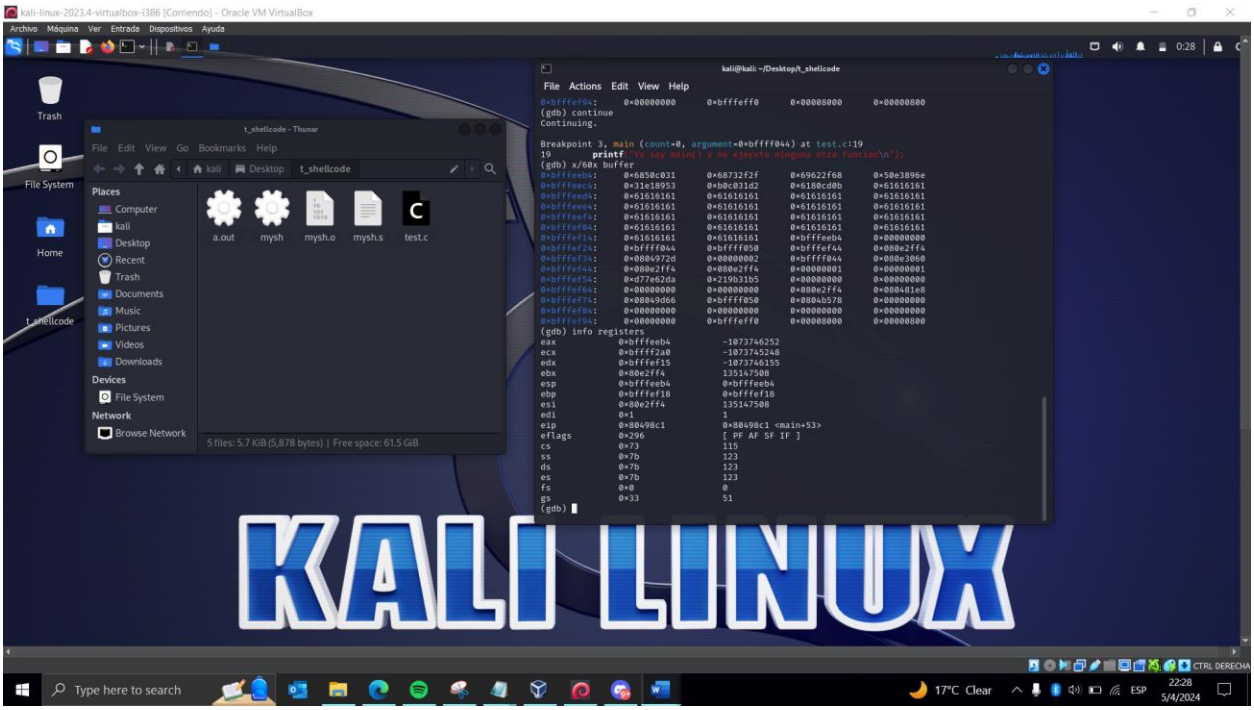
Estado del bufer en el primer breakpoint:



Estado del buffer en el seguro y tercer breakpoint. En el tercero ya se ejecutó el strcopy.



Revisión del estado de los registros para confirmar que el stackpointer apunte a las instrucciones inyectadas.



Finalización del programa. El shellcode fue exitoso y se ganó acceso al bash. Se probó con un echo $$.