Respuestas checkpoint 4 (Validate Key)

1. -Sí, pues tenemos acceso al RIP de la llamadora que está guardado en la pila.

También, pues podríamos volver a una dirección anterior y conocer dicho contexto.

Para hallar la clave nos serviría encontrar cierta funcion que compare la clave ingresada con aquella correcta. Como se trata de una variable local, muy posiblemente sea parte del contexto de alguna funcion que la verifica.

1. File do\_stuff.c:

9: void do\_stuff(int);

3: void encode(char \*, char \*);

Non-debugging symbols:

0x00001000 \_init

0x000010e0 \_\_cxa\_finalize@plt

0x000010f0 strncpy@plt

0x00001100 puts@plt

0x00001110 inet\_ntoa@plt

0x00001120 \_\_stack\_chk\_fail@plt

0x00001130 printf@plt

0x00001140 ioctl@plt

0x00001150 close@plt

0x00001160 strcmp@plt

0x00001170 if\_nameindex@plt

0x00001180 if\_freenameindex@plt

0x00001190 socket@plt

0x000011a0 \_start

0x000011d0 deregister\_tm\_clones

0x00001200 register\_tm\_clones

0x00001240 \_\_do\_global\_dtors\_aux

0x00001280 frame\_dummy

0x00001289 do\_some\_more\_stuff

0x000012c8 do\_some\_stuff

0x00001308 main

0x000014e0 \_\_libc\_csu\_init

0x00001550 \_\_libc\_csu\_fini

0x00001558 \_fini