DESACTIVANDO bomba_CRC_2019

Daniel Monjas Miguélez

23 de diciembre de 2019

1. Pasos para desactivar bomba_CRC_2019

Primero establecemos un breakpoint en el main y ejecutamos con nexti hasta que la bomba explote. Siguiendo este esquema llegamos a la direccion **0x565559cb**, que es donde se produce la primera llamada a boom. Fijándonos en el código ensamblador de la bomba podemos ver que en las instrucciones previas al call <boom>se produce un **cmpl $0x2, -0xd8(%ebp)**, luego pondremos un breakpoint en el cmpl y observaremos los valores que tenga en dicho punto la dirección dada. Con modificar la dirección dada para que no contenga 2, la bomba pasa a estar desactivada.

2. Pasos para obtener contraseña y código

Si nos fijamos un poco en el código vemos que hay varios strncmp luego puede ser que haya más de una constraseña. Vamos a ir leyendo el código en ensamblador de arriba abajo y lo primero que encontramos es que lo primero que se hace es comparar las longitudes de la constraseña esperada y la introducida. Luego al llegar a la dirección **0x565558c6**, observamos que se hace un cmp entre las dos direcciones donde se han almacenado las longitudes de las contraseñas, si no son iguales se pone 1 en la direccion **-0xd8(%ebp)**, lo que más adelante implicara la explosión de la bomba. Un poco más abajo se produce el primer strncmp, donde si la contraseña no coincide se continua ejecutando normal en vez de usar el jne(esto se debe a que test activa el flag ZF y jne sólo salta si este flag es distinto de 1, que lo es en este caso pues %eax contiene 1 tras el test luego el flag ZF estará a 0), entonces sabemos que la dirección **-0xd4(%ebp)**, contiene la contraseña que nos interesa, luego la imprimimos con print (char*)int(direccion), si bien luego hay otro strcmp y la contraseña con la que se compara entonces podría ser válida no nos sirve porque si el primer strcmp falla entonces se almacena 1 en la dirección que nos interese y dicho 1 no se modifica, lo que más adelante conllevará que explote la bomba. Por último nos queda adivinar el código, el cual esta almacenado en la direccion **-0xc0(%ebp)**, esto se debe porque el cmp que compara el código introducido y el valido se realiza justo después de la llamada a scanf, y si la comparación falla se almacena 2 en la dirección que nos interesa y esto hará que reviente después. Si probamos con las contraseña y el código de las direcciones mencionadas la bomba se desactiva. Luego finalmente llegamos a la conclusión de que la contraseña es **contraseña=Introduce la**, y el código es **código=100**. Quedando así completamente desactivada la bomba.