DESACTIVANDO BOMBA_DMM

Daniel Monjas Miguélez

23 de diciembre de 2019

1. Pasos para desactivar bomba_dmm

Como se hace en otros casos lo primero será colocar un breakpoint en el main y seguir con la instrucción *nexti* hasta que la bomba explote. Llegamos a la dirección **0x56555663**, donde se produce la primera explosión de la bomba. Nos fijaremos en el código desensamblado de la bomba con **objdump -d <nombre_bomba>**. Viendo el código ensamblador vemos que justo antes de la llamada a la función <boom>se produce una llamada a **strcmp** y un **test %eax, %eax**, donde se compara lo introducido con la contraseña esperada, y si no coinciden la bomba explota. Pondremos en el test un breakpoint y al llegar haremos **set $eax=0**.

Pasada la primera llamada de boom volvemos a hacer nexti hasta que la bomba reviente. Pero curiosamente la bomba vuelve a reventar en la misma dirección que lo hizo en la ocasión anterior. Al fijarnos en las ultimas direcciones por las que pasa nexti podemos fijarnos que justo antes de volver a la llamada de boom se hace un salto desde la dirección **0x565556e8**. Este salto se produce justo después del scanf del código y su posterior comparación con el esperado por el programa. Lo que haremos será establecer un breakpoint en el cmp que hay justo antes del jne. Al alcanzar este último breakpoint usamos el comando **info all-registers**, y nos fijamos en el contenido del registro %eax, y entonces modificamos el contenido de la dirección -0x94(%ebp), para que contenga el código que se encuentra en %eax, que es el código que espera el programa.

2. Pasos para obtener la contraseña

Como ya hemos dicho el código está en el último cmp en el registro %eax, luego con info all-registers podemos conocer cual es el valor del código. Por otro lado para obtener el valor de la contraseña usaremos ltrace -i <programa>, que nos mostrará por pantalla con que cadena de caracteres se hace el strncmp. La otra forma es rastrear hasta el fgets, ver que justo después se hace un strcmp y que antes de este se empujan a la pila las dos direcciones que se van a comparar, una desde registro y la otra desde memoria, si imprimimos con print (char*)(registro) lo que hay en el registro **%edi**, que es donde se encuentra en este caso, tendremos acceso a la contraseña original de la bomba. Usando lo anteriormente puesto se llega a la conclusión de que la constraseña es **suspensocom** y el código es **110920**