Estructura de Computadores - Entrega 3

Yábir García Benchakhtir

26 de diciembre de 2017

1. Tareas realizadas

En esta práctica he construido y encontrado las claves de mi propia bomba. Además he desactivado la bomba de mi compañera Patricia Cordoba y la bomba que aparece en *SWAD* con el nombre de *NBA*.

2. Bomba realizada

Junto a este documento se acompaña la bomba realiza en *C*. Los datos para desactivarla son:

- Contraseña: *Q..W.r*
- Pin: *8746*

2.1. Pasos para la desactivación

Usando *gdb* abrimos el binario de nuestra bomba y ejecutamos la orden *disas* para comprobar las instrucciones de la bomba.

Si observamos el código vemos que se tras leer la entrada se comprueba la longitud y después se llama a la función *boom*.

```
1  0x56555808 <+135>:   call   0x56555560 <strlen@plt>
2  0x5655580d <+140>:   add    $0x10,%esp
3  0x56555810 <+143>:   cmp    %eax,%esi
4  0x56555812 <+145>:   je     0x56555819 <main+152>
5  0x56555814 <+147>:   call   0x565556dd <boom>
6  0x56555819 <+152>:   movl   $0x0,-0x94(%ebp)
```

Si comprobamos el contenido de los registros comprobamos que solo esta el tamaño de la contraseña que no es lo que buscabamos pero es información relevante. En este caso sabemos que la contraseña tiene 6 caracteres.

Cerca de esta zona en el código tenemos una linea donde movemos contendio de *%ebp* a *%eax*, nos hace sospechar que pueda estar moviendo la contraseña. Añadiendo un break en esta linea e imprimiento el contenido de los registros obtenemos:

```
(gdb) info reg
eax            0x0     0
ecx            0x8     8
edx            0x56557008      1448439816
ebx            0x56556fb8      1448439736
esp            0xffffced0      0xffffced0
ebp            0xffffcf68      0xffffcf68
esi            0x7     7
edi            0xf7fb1000      -134541312
eip            0x56555831      0x56555831 <main+176>
eflags         0x202   [ IF ]
cs             0x23    35
ss             0x2b    43
ds             0x2b    43
es             0x2b    43
fs             0x0     0
gs             0x63    99
(gdb) x/s \$edx
0x56557008 <password>:          "Q..W.r\n"
```

De esta manera ya conocemos la contraseña de la bomba. Consultando de nuevo el código del programa observamos la linea:

```
0x565558c3 <+322>: call 0x56555580 <__isoc99_scanf@plt>
```

donde realiza la lectura desde el teclado del código. Mirando cerca de esta instrucción observamos como en el caso de la contraseña:

```
=> 0x565558d1 <+336>: mov     0x58(\%ebx),\%eax
```

Si imprimimos el contenido de los registros obtenemos:

```
eax            0x222a  8746
ecx            0x1     1
edx            0x913   2323
ebx            0x56556fb8      1448439736
esp            0xffffced0      0xffffced0
ebp            0xffffcf68      0xffffcf68
esi            0x7     7
edi            0xf7fb1000      -134541312
eip            0x565558d7      0x565558d7 <main+342>
eflags         0x282   [ SF IF ]
cs             0x23    35
ss             0x2b    43
ds             0x2b    43
es             0x2b    43
fs             0x0     0
gs             0x63    99
```

donde en *eax* tenemos el código de la bomba.

3. Bomba NBA

Usando la herramienta *ghex* comprobamos que hay tres cadenas de texto que pueden ser la contraseña pero no sabemos cual de ellas puede ser. En concreto son: *Oh, castitas lilium*, *Esta es la clave!!* y

Miauuu.

En la dirección *0x08048806* mueve la contraseña a los registros en este caso es *Oh, castitas lilium.* Las otras dos cadenas las compara en las direcciones *0x804b030* y *0x080487ac.* En el caso de las otras dos cadenas de ser una de ellas llama a la función *¡f1_ew¿* que nos muestra en pantalla *miau.*

Observando el código vemos:

```
0x08048880 <+575>: mov     0x804b064,\%eax
0x08048885 <+580>: cmp     \%eax,\%edx
```

si en esta dirección imprimos los registros vemos:

```
eax            0x406    1030
ecx            0x1      1
edx            0x406    8888
ebx            0x0      0
esp            0xffffcec0       0xffffcec0
ebp            0xffffcf68       0xffffcf68
esi            0x1      1
edi            0xf7fb1000       -134541312
eip            0x8048885        0x8048885 <main+580>
eflags         0x246    [ PF ZF IF ]
cs             0x23     35
ss             0x2b     43
ds             0x2b     43
es             0x2b     43
fs             0x0      0
gs             0x63     99
```

donde en *eax* tenemos el pin y en *edx* está el que hemos metido nostros.

4. Bomba de Patricia Cordoba

Los datos de esta bomba son:

- Contraseña: *t...t...*
- Pin: *4444*

Los pasos de manera esquematica han sido:

- Añadir break en main.
- Avanzar hasta que nos pida la contraseña.
- En la instrucción *0x0804877f* vemos un push extraño cerca de donde hemos introducido la contraseña. Si imprimimos su contenido vemos:

  ```
  (gdb) x/s 0x804a0a5
  0x804a0a5 <lalala>: "t...t...\n"
  ```

- En la instrucción *0x0804884d* ya hemos introducido el codigo.
- Vemos una comparación en *0x08048853.*
- Vemos que accede a una posición con aritemética de punteros.
- Hacemos *p (int)($ebp-140)* 140 se corresponde con 0x8c. Así obtenemos el código de la bomba, en este caso, 4444.