Documentación
PRÁCTICA 4

Estructura de computadores

UNIVERSIDAD
DE GRANADA

Fernández Mertanen, Jonathan

Índice

Bomba 1 (bomba_yacine)

Tiempo estimado de resolución: 35 min

Contraseña: tupac

Para la obtención de la contraseña he comprobado los argumentos de la función strcmp, la cual recibe 2 cadenas. En este caso, la primera cadena es “atd” (%rdi) que se asemeja a lo que he introducido por el teclado (“asd”), y la segunda cadena es “tvpbc” (%rsi). Se observa que se realiza algún tipo de encriptación con una función llamada codificación:

```
0x0000000000400809 main+94   callq  0x400796 <codificacion>
```

Analizando su funcionamiento:

```
0x0000000000400796 codificacion+0  movzbl 0x1(%rdi),%eax
0x000000000040079a codificacion+4  add    $0x1,%eax
0x000000000040079d codificacion+7  mov    %al,0x1(%rdi)
0x00000000004007a0 codificacion+10 movzbl 0x3(%rdi),%eax
0x00000000004007a4 codificacion+14 add    $0x1,%eax
0x00000000004007a7 codificacion+17 mov    %al,0x3(%rdi)
0x00000000004007aa codificacion+20 retq
```

Vemos que lo que hace es sumar 1 al segundo y cuarto carácter de la cadena, de esta manera, la cadena “aaaa” codificada sería “abab”.
Transformando de manera inversa al algoritmo de codificación la cadena antes obtenida, tenemos que “tvpbc” -> “tupac”.

Pin: 0

```
0x0000000000400895 main+234 add    $0x4,%eax
0x0000000000400898 main+237 cmp    0x2007ca(%rip),%eax        # 0x601068
<encriptado>
```

Antes de realizar la comparación de pins, entre el tecleado y <encriptado>, se le suma 4 a el pin introducido desde teclado.
<encriptado> tiene almacenado el número 4, por lo que la comparación que se realiza es introducido+4 == 4. Para que esta condición sea verdadera, introducido tiene que ser igual a 0.

```
jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Yacine$ ./bomba_yacine
Introduce la contraseÃ±a: tupac
Introduce el pin: 0

        bomba desactivada

jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Yacine$
```

Cambio de contraseña y pin

La contraseña ya encriptada se encuentra almacenada en 0x60106c.
El pin se encuentra almacenado en 0x601068.
Modificando ambas direcciones, cambiaremos las credenciales que nos piden para desactivar la bomba.
Queremos que la contraseña acepte “hola” por lo que debemos modificar la dirección y guardar la cadena pero ya encriptada, ya que el programa no la encripta en la ejecución.
“hola” -> “hplb” (con su respectivo salto de línea “hplb\n”)
El pin que queremos que acepte es 10, por lo que deberemos modificar <encriptado> para que almacene 14 (10-4).

```
>>> set{char[6]}0x60106c="hplb\n"
>>> set{int}0x601068=14
```

```
jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Yacine$ ./bomba_yacine
Introduce la contraseÃ±a: hola
Introduce el pin: 10

        bomba desactivada

jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Yacine$
```

Bomba 2 (bombaSara)

Tiempo estimado de resolución: 15 min

Contraseña: latarara

En este caso, la contraseña se almacena en 0x601068 sin encriptar, por lo que se puede consultar y modificar fácilmente.

```
0x00000000004007c0 main+101 lea    0x2008a1(%rip),%rsi        # 0x601068
<password>
0x00000000004007c7 main+108 callq  0x4005d0 <strncmp@plt>
```

```
>>> x/1sb 0x601068
0x601068 <password>:    "latarara\n"
```

Pin: 2018

En esta bomba, se suma 8 al passcode, y después se compara. Éste está almacenado en 0x601060 y tiene un valor de 2026, por lo que el pin es 2026-8 = 2018.

```
<main+234>      add     $0x8,%eax
<main+237>      cmp     0x200812(%rip),%eax        # 0x601060 <passcode>
```

```
jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Sara$ ./bombaSara

Introduce la contraseÃ±a: latarara

Introduce el pin: 2018

Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·
Â·Â·Â· bomba desactivada Â·Â·Â·
Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·

jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Sara$
```

Cambio de contraseña y pin

Debemos proceder de la misma manera que en la bomba anterior, siendo la password más simple, ya que no está codificada.
Pondremos las mismas credenciales (hola y 10).

```
>>> set {char[6]}0x601068="hola\n"
>>> set {int}0x601060=18
```

```
jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Sara$ ./bombaSara

Introduce la contraseÃ±a: hola

Introduce el pin: 10

Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·
Â·Â·Â· bomba desactivada Â·Â·Â·
Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·

jonathan@jonathan-K55A:~/Documentos/EC PR/PR4/Sara$
```