Adrián de la Torre Rodríguez 2ºA grupo A2

RESOLUCIÓN BOMBAS PRÁCTICA 4b

BOMBA: bombaProf5_06

AVERIGUACIÓN DE LA CONTRASEÑA Y EL CÓDIGO

Contraseña: `plLFowMY`

Código: `8658`

Para averiguar la contraseña hay que irse antes de la primera llamada a boom donde se llama a la función strncmp. Esta función compara dos cadenas y devuelve true si son iguales. Hay que mirar que argumentos se le pasan puesto que uno de ellos es la contraseña que queremos averiguar. En este caso, se pasa como segundo argumento: `movl $0x804a02c,0x4(%esp)`
Mueve esa posición de memoria a cuatro por encima de esp. Si hacemos un volcado de esa dirección:

Data > Memory

Examine 1 string bytes from 0x804a02c

Obtenemos:

`0x804a02c <password>: "plLFowMY\n"`

Esa es la contraseña que estamos buscando.

Ahora vamos a averiguar el código. Para ello, hay que irse otra vez antes de la siguiente llamada a boom, ahora hace una comprobación de una dirección de memoria con lo que hemos introducido: `cmp 0x804a038,%eax` . Si son iguales se activa el bit de igualdad y se salta

la función boom. Vamos a ver que se almacena en `0x804a038`.

Data > Memory

Examine 5 hex bytes from 0x804a038

Obtenemos:

```
0x804a038 <passcode>: 0xd2 0x21 0x00 0x00 0x00
```

Nos quedamos con los dos primeros números en hexadecimal, que corresponden al código entero que estamos buscando. Hay que tener cuidado porque están en little endian por lo que el numero que buscamos es: `21D2`. Este número en decimal corresponde con el `8658`.

Con todo esto ya hemos averiguado la contraseña y el código de la bomba, lo que nos facilitará cambiarlos después con el ghex.

CAMBIO DE LAS CONTRASEÑAS

Para cambiar la contraseña abrimos la bomba con el ghex y le damos a buscar la contraseña: `plLFowMY`. Vemos que nos muestra en la parte derecha la contraseña resaltada en rojo. Ahora solo basta con pinchar en el primer carácter y escribir encima la nueva contraseña, yo por ejemplo voy a poner `abracada`.

Para cambiar el código tenemos que buscar los números hexadecimales en little endian que obtuvimos anteriormente. Se buscan de la misma manera, solo que esta vez se busca en la parte hexadecimal del buscador. Vemos que vuelven a aparecer resaltados en rojo. Para cambiar este código, paso a hexadecimal otro código cualquiera, por ejemplo `7777: 1e61`. El número obtenido en hexadecimal hay que pasarlo a little endian: `61 1e`. Finalmente hay que escribir este número encima de donde estaba resaltado.

La bomba consta de nuevas contraseñas y la próxima que ejecutemos el programa, para desactivar la bomba habrá que introducir `abracada` y `7777`.

BOMBA: bombaProf5_29

AVERIGUACIÓN DE LA CONTRASEÑA Y EL CÓDIGO

Contraseña: `yyMCLtNs`

Código: `4885`

Para averiguar la contraseña hay que irse antes de la primera llamada a boom donde se llama a la función strncmp. Esta función compara dos cadenas y devuelve true si son iguales. Hay que mirar que argumentos se le pasan puesto que uno de ellos es la contraseña que queremos averiguar. En este caso, se pasa como segundo argumento: `movl $0x804a02c,0x4(%esp)`
Mueve esa posición de memoria a cuatro por encima de esp. Si hacemos un volcado de esa dirección:

Data > Memory

Examine 1 string bytes from 0x804a02c

Obtenemos:

`0x804a02c <password>: "yyMCLtNs\n"`

Esa es la contraseña que estamos buscando.

Ahora vamos a averiguar el código. Para ello, hay que irse otra vez antes de la siguiente llamada a boom, ahora hace una comprobación de una dirección de memoria con lo que hemos introducido: `cmp 0x804a038,%eax` . Si son iguales se activa el bit de igualdad y se salta la función boom. Vamos a ver que se almacena en `0x804a038`.

Data > Memory

Examine 5 hex bytes from 0x804a038

Obtenemos:

```
0x804a038 <passcode>: 0x15 0x13 0x00 0x00 0x00
```

Nos quedamos con los dos primeros números en hexadecimal, que corresponden al código entero que estamos buscando. Hay que tener cuidado porque están en little endian por lo que el numero que buscamos es: `1315`. Este número en decimal corresponde con el `4885`.

Con todo esto ya hemos averiguado la contraseña y el código de la bomba, lo que nos facilitará cambiarlos después con el ghex.

CAMBIO DE LAS CONTRASEÑAS

Para cambiar la contraseña abrimos la bomba con el ghex y le damos a buscar la contraseña: `yyMCLtNs`. Vemos que nos muestra en la parte derecha la contraseña resaltada en rojo. Ahora solo basta con pinchar en el primer carácter y escribir encima la nueva contraseña, yo por ejemplo voy a poner `ebrecede`.

Para cambiar el código tenemos que buscar los números hexadecimales en little endian que obtuvimos anteriormente. Se buscan de la misma manera, solo que esta vez se busca en la parte hexadecimal del buscador. Vemos que vuelven a aparecer resaltados en rojo. Para cambiar este código, paso a hexadecimal otro código cualquiera, por ejemplo `4444: 115C`. El número obtenido en hexadecimal hay que pasarlo a little endian: `5C 11`. Finalmente hay que escribir este número encima de donde estaba resaltado.

La bomba consta de nuevas contraseñas y la próxima que ejecutemos el programa para desactivar la bomba habrá que introducir `ebrecede` y `4444`.