
Aouadj Moncef

G1

Exercice 3 :

1*

```
#include <stdlib.h>

char* tab;

int main()
{

arr = malloc(16384* sizeof(char));

for (int i=0; i<16384; i++) arr[i] = '0';

return 0;

}
```

2*

/----- PROTECTION CONTRE L'ÉCRITURE -----/

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/mman.h>
#include <malloc.h>

char* arr;
char* alloc;
int pagesize ;

int main()
{

alloc = malloc(1024L * 1024L );

arr = malloc(16384* sizeof(char));

for (int i=0; i<16384; i++) arr[i] = '0';

pagesize = sysconf(_SC_PAGE_SIZE);
```

```
printf("Tête du tableau: 0x%lx\n", (long) arr);

arr = memalign(pagesize, 4 * pagesize);

mprotect(arr+ pagesize, 2 * pagesize, PROT_WRITE);

arr[4098] = '1'; /*impossible, car la mémoire est protégée contre
l'écriture*/

sprintf(alloc, "cat /proc/%d/maps", getpid());
system(alloc);
return 0;

}
```

/----- PROTECTION CONTRE LA LECTURE -----/

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/mman.h>
#include <malloc.h>

char* arr;
char* alloc;
int pagesize;

int main()
{

alloc = malloc(1024L * 1024L );

arr = malloc(16384* sizeof(char));

for (int i=0; i<16384; i++) arr[i] = '0';

pagesize = sysconf(_SC_PAGE_SIZE);

printf("Tête du tableau: 0x%lx\n", (long) arr);

arr = memalign(pagesize, 4 * pagesize);

mprotect(arr+ pagesize, 2 * pagesize, PROT_READ);

printf ("%c\n", arr[4098]); /*impossible, car la mémoire est protégée
contre la lecture*/
```

```
sprintf(alloc, "cat /proc/%d/maps", getpid());
system(alloc);
return 0;

}
```

3*

/----- Avant la protection contre Lecture -----/

Tête du tableau: 0x55d931a582a0

0

```
55d930da2000-55d930da3000 r--p 00000000 08:01 692340
/home/a.out
55d930da3000-55d930da4000 r-xp 00001000 08:01 692340
/home/a.out
55d930da4000-55d930da5000 r--p 00002000 08:01 692340
/home/a.out
55d930da5000-55d930da6000 r--p 00002000 08:01 692340
/home/a.out
55d930da6000-55d930da7000 rw-p 00003000 08:01 692340
/home/a.out
55d931a58000-55d931a79000 rw-p 00000000 00:00 0
[heap]
7f4bb15fa000-7f4bb16fb000 rw-p 00000000 00:00 0
7f4bb16fb000-7f4bb171d000 r--p 00000000 00:a7 776003
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7f4bb171d000-7f4bb1895000 r-xp 00022000 00:a7 776003
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7f4bb1895000-7f4bb18e3000 r--p 0019a000 00:a7 776003
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7f4bb18e3000-7f4bb18e7000 r--p 001e7000 00:a7 776003
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7f4bb18e7000-7f4bb18e9000 rw-p 001eb000 00:a7 776003
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7f4bb18e9000-7f4bb18ef000 rw-p 00000000 00:00 0
7f4bb18fe000-7f4bb18ff000 r--p 00000000 00:a7 775981
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7f4bb18ff000-7f4bb1922000 r-xp 00001000 00:a7 775981
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7f4bb1922000-7f4bb192a000 r--p 00024000 00:a7 775981
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7f4bb192b000-7f4bb192c000 r--p 0002c000 00:a7 775981
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7f4bb192c000-7f4bb192d000 rw-p 0002d000 00:a7 775981
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7f4bb192d000-7f4bb192e000 rw-p 00000000 00:00 0
```

```
7ffc7742d000-7ffc7744e000 rw-p 00000000 00:00 0
[stack]
7ffc7759f000-7ffc775a2000 r--p 00000000 00:00 0
[vvar]
7ffc775a2000-7ffc775a3000 r-xp 00000000 00:00 0
[vdso]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0
[vsyscall]
```

/----- Après la protection contre Lecture -----/

Tête du tableau: 0x55b942f602a0

```
55b942249000-55b94224a000 r--p 00000000 08:01 699831
/home/a.out
55b94224a000-55b94224b000 r-xp 00001000 08:01 699831
/home/a.out
55b94224b000-55b94224c000 r--p 00002000 08:01 699831
/home/a.out
55b94224c000-55b94224d000 r--p 00002000 08:01 699831
/home/a.out
55b94224d000-55b94224e000 rw-p 00003000 08:01 699831
/home/a.out
55b942f60000-55b942f66000 rw-p 00000000 00:00 0
[heap]
55b942f66000-55b942f68000 r--p 00000000 00:00 0
[heap]
55b942f68000-55b942f81000 rw-p 00000000 00:00 0
[heap]
7fd207baa000-7fd207cab000 rw-p 00000000 00:00 0
7fd207cab000-7fd207ccd000 r--p 00000000 00:256 775932
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7fd207ccd000-7fd207e45000 r-xp 00022000 00:256 775932
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7fd207e45000-7fd207e93000 r--p 0019a000 00:256 775932
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7fd207e93000-7fd207e97000 r--p 001e7000 00:256 775932
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7fd207e97000-7fd207e99000 rw-p 001eb000 00:256 775932
/usr/lib/x86_64-linux-gnu/libc-2.31.so
7fd207e99000-7fd207e9f000 rw-p 00000000 00:00 0
7fd207eae000-7fd207eaf000 r--p 00000000 00:256 775909
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7fd207eaf000-7fd207ed2000 r-xp 00001000 00:256 775909
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7fd207ed2000-7fd207eda000 r--p 00024000 00:256 775909
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7fd207edb000-7fd207edc000 r--p 0002c000 00:256 775909
/usr/lib/x86_64-linux-gnu/ld-2.31.so
```

7fd207edc000-7fd207edd000 rw-p 0002d000 00:256 775909
/usr/lib/x86_64-linux-gnu/ld-2.31.so
7fd207edd000-7fd207ede000 rw-p 00000000 00:00 0
7ffd40cd8000-7ffd40cf9000 rw-p 00000000 00:00 0
[stack]
7ffd40df8000-7ffd40dfb000 r--p 00000000 00:00 0
[vvar]
7ffd40dfb000-7ffd40dfc000 r-xp 00000000 00:00 0
[vdso]
ffffffff600000-ffffffff601000 --xp 00000000 00:00 0
[vsyscall]