1.1 (voir top.txt)

```
top
```

1.2 (voir strace_1_2.txt)

```
strace -e open ps```
```

'ps' ouvre les fichiers: - dossier de chaque processus ('/proc/*') - '/proc/meminfo' - des bibliothèques dynamiques ('/lib64') - '/proc/tty/drivers'

1.3 (voir 'strace_1_3.txt')

```
[romain.pereira@vm0 tp]$ strace -c ps -elf
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 37.86    0.004293           8       506           read
 22.48    0.002549           5       485        12 open
 15.46    0.001753           5       343         9 stat
 11.15    0.001264           3       476           close
  4.45    0.000505           5       108           write
  3.01    0.000341           4        85           mmap
  2.10    0.000238           5        47           mprotect
  0.87    0.000099           2        42           fstat
  0.78    0.000089           5        17           munmap
  0.41    0.000047           2        24           rt_sigaction
  0.28    0.000032           8         4         1 readlink
  0.26    0.000030          15         2           statfs
  0.21    0.000024          12         2           socket
  0.19    0.000022           7         3         2 access
  0.16    0.000018           9         2         2 connect
  0.05    0.000006           2         3           brk
  0.05    0.000006           3         2           ioctl
  0.04    0.000004           1         3           lseek
  0.04    0.000004           2         2           getdents
  0.02    0.000002           2         1           rt_sigprocmask
  0.02    0.000002           2         1           uname
  0.02    0.000002           2         1           getrlimit
  0.02    0.000002           2         1           geteuid
  0.02    0.000002           2         1           arch_prctl
  0.02    0.000002           2         1           futex
  0.02    0.000002           2         1           set_tid_address
  0.02    0.000002           2         1           set_robust_list
  0.00    0.000000           0         1           execve
  0.00    0.000000           0         1           openat
------ ----------- ----------- --------- --------- ----------------
100.00    0.011340                  2166        26 total
```

=> 2166 appels systèmes

1.4 (voir 'strace_1_4.txt')

```
strace -c lsof
```

Liste des fichiers ouverts

```
[romain.pereira@vm0 tp]$ strace -e open lsof
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
open("/lib64/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib64/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
open("/lib64/libpcre.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib64/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
open("/lib64/libpthread.so.0", O_RDONLY|O_CLOEXEC) = 3
open("/dev/null", O_RDWR)               = 3
open("/usr/lib/locale/locale-archive", O_RDONLY|O_CLOEXEC) = 3
open("/", O_RDONLY)                     = 3
open("/proc/1601/fdinfo/3", O_RDONLY)   = 4
open("/proc/mounts", O_RDONLY)          = 3
--- SIGALRM {si_signo=SIGALRM, si_code=SI_KERNEL} ---
```

Les '.so' correspondent aux bibliothèques dynamiques chargées par le programme

Pour lister et compter les appels aux bibliothèques externes:

```
ltrace -c lsof -e /mnt
```

Ce qui donne

```
% time     seconds  usecs/call     calls      function
------ ----------- ----------- --------- --------------------
 69.59    7.141255     3570627         2 __libc_start_main
  4.10    0.420334          98      4275 strlen
  3.65    0.374757          98      3816 snprintf
  3.07    0.314779         452       696 read
  2.11    0.216418          99      2172 __snprintf_chk
  1.99    0.203838          98      2078 __ctype_b_loc
  1.88    0.193144         208       928 write
  1.77    0.181623          97      1858 malloc
  1.16    0.119393          99      1204 _IO_putc
  1.12    0.114518         111      1025 close
  1.11    0.113465          97      1160 strncpy
  0.87    0.089395          98       912 mblen
  0.80    0.082570          97       846 strtol
  0.69    0.071295          97       728 __errno_location
  0.68    0.070231         103       677 readdir64
  0.60    0.061151         109       561 fgets

  0.52    0.052885         113       464 alarm
  0.51    0.052427         112       464 signal
  0.47    0.048723          98       496 strerror
```

```
  0.47    0.048585         118       411 readlink
  0.35    0.035488         124       284 fopen64
  0.28    0.028722         118       243 opendir
  0.27    0.027975         118       236 fclose
  0.24    0.024258          97       248 strtoull
  0.22    0.022578          97       232 _setjmp
  0.21    0.021050          98       214 setvbuf
  0.20    0.020440         107       190 __printf_chk
  0.18    0.018809          97       193 strcasecmp
  0.13    0.013579         115       118 closedir
  0.13    0.013084         115       113 __xstat64
  0.12    0.012761          97       131 strrchr
  0.09    0.009334        1166         8 getpwuid
  0.09    0.008799          96        91 __strncpy_chk
  0.09    0.008733          97        90 strcmp
  0.08    0.008242          98        84 strncmp
  0.04    0.003962          99        40 strchr
  0.04    0.003937          96        41 __ctype_get_mb_cur_max
  0.03    0.003046          98        31 realloc
  0.02    0.002527          97        26 strtoul
  0.00    0.000393          98         4 free
  0.00    0.000384         384         1 fork
  0.00    0.000284         284         1 qsort
  0.00    0.000238         119         2 open64
  0.00    0.000234         117         2 pipe
  0.00    0.000217         217         1 setlocale
  0.00    0.000206         103         2 calloc
  0.00    0.000124         124         1 __lxstat64
  0.00    0.000120         120         1 getgid
  0.00    0.000119         119         1 getuid
  0.00    0.000117         117         1 getdtablesize
  0.00    0.000114         114         1 getegid
  0.00    0.000113         113         1 umask
  0.00    0.000112         112         1 geteuid
  0.00    0.000112         112         1 lseek64
  0.00    0.000111         111         1 strncasecmp
  0.00    0.000111         111         1 getpagesize
  0.00    0.000104         104         1 is_selinux_enabled
  0.00    0.000103         103         1 getpid
```

=> La fonction la plus appelé est 'strlen()' qui calcul la longueur d'une chaîne de caractères

2.1

```
[romain.pereira@vm0 tp]$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 33151
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
```

```
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 4096
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

La taille de la pile des processus est réglé sur 8192 kbytes

Voici 2 programmes qui font un dépassement de pile:

```
void main() {
    char c[8192 * 1024];
}
```

```
void main() {
    main();
}
```

Compilation puis execution, le programme plante

```
[romain.pereira@vm0 tp]$ gcc stackoverflow.c
[romain.pereira@vm0 tp]$ ./a.out
Erreur de segmentation
```

=> Il y a eu un dépassement de pile

Correction: Dans le cas d'une récursion infini : mettre une condition sortie dans la récursion

Dans le cas d'une pile trop petite, on peut aggrandir dynamiquement la taille de la pile:

```
ulimit -s {TAILLE_EN_KBYTES}
```

3.1

```
[romain.pereira@vm0 tp]$ ls -l
total 72
drwxrwxr-x. 2 romain.pereira   174 26 nov.  16:38 .
drwx------. 4 romain.pereira   137 26 nov.  16:36 ..
-rwxrwxr-x. 1 romain.pereira  8552 26 nov.  16:37 binaire
-rwxrwxr-x. 1 romain.pereira  9856 26 nov.  16:37 binaireg
```

Le binaire compilé avec le flag *-g* est plus volumineux que celui sans.

On observe les binaires à l'aide de l'utilitaire **readelf**

```
[romain.pereira@vm0 tp]$ readelf -s binaire

Table de symboles « .dynsym » contient 5 entrées :
   Num:    Valeur          Tail Type    Lien   Vis      Ndx Nom
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND
__libc_start_main@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND exit@GLIBC_2.2.5 (2)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND usleep@GLIBC_2.2.5 (2)

Table de symboles « .symtab » contient 67 entrées :
   Num:    Valeur          Tail Type    Lien   Vis      Ndx Nom
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000400238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000400254     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000400274     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000400298     0 SECTION LOCAL  DEFAULT    4
     5: 00000000004002b8     0 SECTION LOCAL  DEFAULT    5
     6: 0000000000400330     0 SECTION LOCAL  DEFAULT    6
     7: 0000000000400374     0 SECTION LOCAL  DEFAULT    7
     8: 0000000000400380     0 SECTION LOCAL  DEFAULT    8
     9: 00000000004003a0     0 SECTION LOCAL  DEFAULT    9
    10: 00000000004003b8     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000400400     0 SECTION LOCAL  DEFAULT   11
    12: 0000000000400420     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000400460     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000400470     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000400634     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000400640     0 SECTION LOCAL  DEFAULT   16
    17: 0000000000400650     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000400698     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000600e10     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000600e18     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000600e20     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000600e28     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000600ff8     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000601000     0 SECTION LOCAL  DEFAULT   24
    25: 0000000000601030     0 SECTION LOCAL  DEFAULT   25
    26: 0000000000601034     0 SECTION LOCAL  DEFAULT   26
    27: 0000000000000000     0 SECTION LOCAL  DEFAULT   27
    28: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    29: 0000000000600e20     0 OBJECT  LOCAL  DEFAULT   21 __JCR_LIST__
    30: 00000000004004a0     0 FUNC    LOCAL  DEFAULT   14 deregister_tm_clones
    31: 00000000004004d0     0 FUNC    LOCAL  DEFAULT   14 register_tm_clones
    32: 0000000000400510     0 FUNC    LOCAL  DEFAULT   14 __do_global_dtors_aux
    33: 0000000000601034     1 OBJECT  LOCAL  DEFAULT   26 completed.6355
    34: 0000000000600e18     0 OBJECT  LOCAL  DEFAULT   20
__do_global_dtors_aux_fin
    35: 0000000000400530     0 FUNC    LOCAL  DEFAULT   14 frame_dummy
    36: 0000000000600e10     0 OBJECT  LOCAL  DEFAULT   19
__frame_dummy_init_array_
    37: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS source.c
    38: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    39: 00000000004007c8     0 OBJECT  LOCAL  DEFAULT   18 __FRAME_END__
    40: 0000000000600e20     0 OBJECT  LOCAL  DEFAULT   21 __JCR_END__
    41: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
```

```
    42: 0000000000600e18     0 NOTYPE  LOCAL  DEFAULT   19 __init_array_end
    43: 0000000000600e28     0 OBJECT  LOCAL  DEFAULT   22 _DYNAMIC
    44: 0000000000600e10     0 NOTYPE  LOCAL  DEFAULT   19 __init_array_start
    45: 0000000000400650     0 NOTYPE  LOCAL  DEFAULT   17 __GNU_EH_FRAME_HDR
    46: 0000000000601000     0 OBJECT  LOCAL  DEFAULT   24 _GLOBAL_OFFSET_TABLE_
    47: 0000000000400630     2 FUNC    GLOBAL DEFAULT   14 __libc_csu_fini
    48: 0000000000601030     0 NOTYPE  WEAK   DEFAULT   25 data_start
    49: 0000000000400572    51 FUNC    GLOBAL DEFAULT   14 loop
    50: 0000000000601034     0 NOTYPE  GLOBAL DEFAULT   25 _edata
    51: 0000000000400634     0 FUNC    GLOBAL DEFAULT   15 _fini
    52: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND
__libc_start_main@@GLIBC_
    53: 0000000000601030     0 NOTYPE  GLOBAL DEFAULT   25 __data_start
    54: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    55: 0000000000400648     0 OBJECT  GLOBAL HIDDEN    16 __dso_handle
    56: 0000000000400640     4 OBJECT  GLOBAL DEFAULT   16 _IO_stdin_used
    57: 00000000004005c0   101 FUNC    GLOBAL DEFAULT   14 __libc_csu_init
    58: 0000000000601038     0 NOTYPE  GLOBAL DEFAULT   26 _end
    59: 0000000000400470     0 FUNC    GLOBAL DEFAULT   14 _start
    60: 0000000000601034     0 NOTYPE  GLOBAL DEFAULT   26 __bss_start
    61: 00000000004005a5    19 FUNC    GLOBAL DEFAULT   14 main
    62: 000000000040055d    21 FUNC    GLOBAL DEFAULT   14 check
    63: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND exit@@GLIBC_2.2.5
    64: 0000000000601038     0 OBJECT  GLOBAL HIDDEN    25 __TMC_END__
    65: 0000000000400400     0 FUNC    GLOBAL DEFAULT   11 _init
    66: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND usleep@@GLIBC_2.2.5
```

```
[romain.pereira@vm0 tp]$ readelf -s binaireg

Table de symboles « .dynsym » contient 5 entrées :
   Num:    Valeur          Tail Type    Lien   Vis      Ndx Nom
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND
__libc_start_main@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND exit@GLIBC_2.2.5 (2)
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND usleep@GLIBC_2.2.5 (2)

Table de symboles « .symtab » contient 72 entrées :
   Num:    Valeur          Tail Type    Lien   Vis      Ndx Nom
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000400238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000400254     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000400274     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000400298     0 SECTION LOCAL  DEFAULT    4
     5: 00000000004002b8     0 SECTION LOCAL  DEFAULT    5
     6: 0000000000400330     0 SECTION LOCAL  DEFAULT    6
     7: 0000000000400374     0 SECTION LOCAL  DEFAULT    7
     8: 0000000000400380     0 SECTION LOCAL  DEFAULT    8
     9: 00000000004003a0     0 SECTION LOCAL  DEFAULT    9
    10: 00000000004003b8     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000400400     0 SECTION LOCAL  DEFAULT   11
    12: 0000000000400420     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000400460     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000400470     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000400634     0 SECTION LOCAL  DEFAULT   15
```

```
    16: 0000000000400640     0 SECTION LOCAL  DEFAULT   16
    17: 0000000000400650     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000400698     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000600e10     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000600e18     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000600e20     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000600e28     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000600ff8     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000601000     0 SECTION LOCAL  DEFAULT   24
    25: 0000000000601030     0 SECTION LOCAL  DEFAULT   25
    26: 0000000000601034     0 SECTION LOCAL  DEFAULT   26
    27: 0000000000000000     0 SECTION LOCAL  DEFAULT   27
    28: 0000000000000000     0 SECTION LOCAL  DEFAULT   28
    29: 0000000000000000     0 SECTION LOCAL  DEFAULT   29
    30: 0000000000000000     0 SECTION LOCAL  DEFAULT   30
    31: 0000000000000000     0 SECTION LOCAL  DEFAULT   31
    32: 0000000000000000     0 SECTION LOCAL  DEFAULT   32
    33: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    34: 0000000000600e20     0 OBJECT  LOCAL  DEFAULT   21 __JCR_LIST__
    35: 00000000004004a0     0 FUNC    LOCAL  DEFAULT   14 deregister_tm_clones
    36: 00000000004004d0     0 FUNC    LOCAL  DEFAULT   14 register_tm_clones
    37: 0000000000400510     0 FUNC    LOCAL  DEFAULT   14 __do_global_dtors_aux
    38: 0000000000601034     1 OBJECT  LOCAL  DEFAULT   26 completed.6355
    39: 0000000000600e18     0 OBJECT  LOCAL  DEFAULT   20
__do_global_dtors_aux_fin
    40: 0000000000400530     0 FUNC    LOCAL  DEFAULT   14 frame_dummy
    41: 0000000000600e10     0 OBJECT  LOCAL  DEFAULT   19
__frame_dummy_init_array_
    42: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS source.c
    43: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    44: 00000000004007c8     0 OBJECT  LOCAL  DEFAULT   18 __FRAME_END__
    45: 0000000000600e20     0 OBJECT  LOCAL  DEFAULT   21 __JCR_END__
    46: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
    47: 0000000000600e18     0 NOTYPE  LOCAL  DEFAULT   19 __init_array_end
    48: 0000000000600e28     0 OBJECT  LOCAL  DEFAULT   22 _DYNAMIC
    49: 0000000000600e10     0 NOTYPE  LOCAL  DEFAULT   19 __init_array_start
    50: 0000000000400650     0 NOTYPE  LOCAL  DEFAULT   17 __GNU_EH_FRAME_HDR
    51: 0000000000601000     0 OBJECT  LOCAL  DEFAULT   24 _GLOBAL_OFFSET_TABLE_
    52: 0000000000400630     2 FUNC    GLOBAL DEFAULT   14 __libc_csu_fini
    53: 0000000000601030     0 NOTYPE  WEAK   DEFAULT   25 data_start
    54: 0000000000400572    51 FUNC    GLOBAL DEFAULT   14 loop
    55: 0000000000601034     0 NOTYPE  GLOBAL DEFAULT   25 _edata
    56: 0000000000400634     0 FUNC    GLOBAL DEFAULT   15 _fini
    57: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND
__libc_start_main@@GLIBC_
    58: 0000000000601030     0 NOTYPE  GLOBAL DEFAULT   25 __data_start
    59: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    60: 0000000000400648     0 OBJECT  GLOBAL HIDDEN    16 __dso_handle
    61: 0000000000400640     4 OBJECT  GLOBAL DEFAULT   16 _IO_stdin_used
    62: 00000000004005c0   101 FUNC    GLOBAL DEFAULT   14 __libc_csu_init
    63: 0000000000601038     0 NOTYPE  GLOBAL DEFAULT   26 _end
    64: 0000000000400470     0 FUNC    GLOBAL DEFAULT   14 _start
    65: 0000000000601034     0 NOTYPE  GLOBAL DEFAULT   26 __bss_start
    66: 00000000004005a5    19 FUNC    GLOBAL DEFAULT   14 main
    67: 000000000040055d    21 FUNC    GLOBAL DEFAULT   14 check
    68: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND exit@@GLIBC_2.2.5
    69: 0000000000601038     0 OBJECT  GLOBAL HIDDEN    25 __TMC_END__
    70: 0000000000400400     0 FUNC    GLOBAL DEFAULT   11 _init
```

```
    71: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND usleep@@GLIBC_2.2.5
```

On constate qu'il y a 5 symboles de plus lorsque l'on compile avec le flag **-g**