

```

1  gdb run - ARCH
2
3
4  echo 0 | sudo tee /proc/sys/kernel/randomize_va_space
5
6
7
8  student@arch-small CS460_Code_Examples]$ gdb ./bin/dup2_example
9  GNU gdb (GDB) 8.0.1
10 ...
11 Reading symbols from ./bin/dup2_example...done.
12 (gdb) break dup2
13 Breakpoint 1 at 0x860
14 (gdb) break 42
15 Breakpoint 2 at 0xa45: file src/dup2_example.c, line 42.
16 (gdb) break 68
17 Breakpoint 3 at 0xb30: file src/dup2_example.c, line 68.
18 (gdb) set disassemble-next-line on
19 (gdb) run
20 Starting program: /home/student/git/cs460_WithWorkspace/CS460_Code_Examples/bin/dup2_example
21 (gdb) break 42
22 Breakpoint 1 at 0xa45: file src/dup2_example.c, line 42.
23 (gdb) break 68
24 Breakpoint 2 at 0xb30: file src/dup2_example.c, line 68.
25 (gdb) break dup2
26 Breakpoint 3 at 0x860
27 (gdb) set disassemble-next-line on
28 (gdb) run
29 Starting program: /home/student/git/cs460_WithWorkspace/CS460_Code_Examples/bin/dup2_example
30
31 Breakpoint 1, main () at src/dup2_example.c:42
32 42      dup2(fd, STDOUT_FILENO);
33 => 0x0000555555554a45 <main+75>:  8b 85 ec fb ff ff  mov   -0x414(%rbp),%eax
34      0x0000555555554a4b <main+81>:  be 01 00 00 00  mov   $0x1,%esi
35      0x0000555555554a50 <main+86>:  89 c7  mov   %eax,%edi
36      0x0000555555554a52 <main+88>:  e8 09 fe ff ff  callq 0x555555554860 <dup2@plt>
37 (gdb) stepi
38 0x0000555555554a4b 42      dup2(fd, STDOUT_FILENO);
39      0x0000555555554a45 <main+75>:  8b 85 ec fb ff ff  mov   -0x414(%rbp),%eax
40 => 0x0000555555554a4b <main+81>:  be 01 00 00 00  mov   $0x1,%esi
41      0x0000555555554a50 <main+86>:  89 c7  mov   %eax,%edi
42      0x0000555555554a52 <main+88>:  e8 09 fe ff ff  callq 0x555555554860 <dup2@plt>
43 (gdb)
44 0x0000555555554a50 42      dup2(fd, STDOUT_FILENO);
45      0x0000555555554a45 <main+75>:  8b 85 ec fb ff ff  mov   -0x414(%rbp),%eax

```

```

46 0x0000555555554a4b <main+81>: be 01 00 00 00 mov $0x1,%esi
47 => 0x0000555555554a50 <main+86>: 89 c7 mov %eax,%edi
48 0x0000555555554a52 <main+88>: e8 09 fe ff ff callq 0x555555554860 <dup2@plt>
49 (gdb)
50 0x0000555555554a52 42 dup2(fd, STDOUT_FILENO);
51 0x0000555555554a45 <main+75>: 8b 85 ec fb ff ff mov -0x414(%rbp),%eax
52 0x0000555555554a4b <main+81>: be 01 00 00 00 mov $0x1,%esi
53 0x0000555555554a50 <main+86>: 89 c7 mov %eax,%edi
54 => 0x0000555555554a52 <main+88>: e8 09 fe ff ff callq 0x555555554860 <dup2@plt>
55 (gdb) stepi
56 0x0000555555554860 in dup2@plt ()
57 => 0x0000555555554860 <dup2@plt+0>: ff 25 ca 07 20 00 jmpq *0x2007ca(%rip) # 0x555555755030
58 (gdb) x 0x555555755030
59 0x555555755030: 0x55554866
60 (gdb) disas 0x55554866
61 No function contains specified address.
62 (gdb) disas 0x0000555555554866
63 Dump of assembler code for function dup2@plt:
64 => 0x0000555555554860 <+0>: jmpq *0x2007ca(%rip) # 0x555555755030
65 0x0000555555554866 <+6>: pushq $0x3
66 0x000055555555486b <+11>: jmpq 0x555555554820
67 End of assembler dump.
68 (gdb)
69
70
71 (gdb) stepi
72 0x0000555555554866 in dup2@plt ()
73 => 0x0000555555554866 <dup2@plt+6>: 68 03 00 00 00 pushq $0x3
74 (gdb)
75
76
77
78 ((gdb) stepi
79 0x0000555555554866 in dup2@plt ()
80 => 0x0000555555554866 <dup2@plt+6>: 68 03 00 00 00 pushq $0x3
81 (gdb)
82 0x000055555555486b in dup2@plt ()
83 => 0x000055555555486b <dup2@plt+11>: e9 b0 ff ff ff jmpq 0x555555554820
84 (gdb)
85 0x0000555555554820 in ?? ()
86 => 0x0000555555554820: ff 35 e2 07 20 00 pushq 0x2007e2(%rip) # 0x555555755008
87 (gdb)
88 0x0000555555554826 in ?? ()
89 => 0x0000555555554826: ff 25 e4 07 20 00 jmpq *0x2007e4(%rip) # 0x555555755010
90 (gdb)

```

```

91 0x00007ffff7dede10 in _dl_runtime_resolve_xsave () from /lib64/ld-linux-x86-64.so.2
92 => 0x00007ffff7dede10 <_dl_runtime_resolve_xsave+0>: 53 push %rbx
93 (gdb) cont
94 Continuing.
95
96 Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
97 => 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00 mov $0x21,%eax
98 (gdb)
99
100
101 Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
102 => 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00 mov $0x21,%eax
103 (gdb) disas $pc
104 Dump of assembler code for function dup2:
105 => 0x00007ffff7b08c70 <+0>: mov $0x21,%eax
106 0x00007ffff7b08c75 <+5>: syscall
107 0x00007ffff7b08c77 <+7>: cmp $0xffffffffffffffff001,%rax
108 0x00007ffff7b08c7d <+13>: jae 0x7ffff7b08c80 <dup2+16>
109 0x00007ffff7b08c7f <+15>: retq
110 0x00007ffff7b08c80 <+16>: mov 0x2c9179(%rip),%rcx # 0x7ffff7dd1e00
111 0x00007ffff7b08c87 <+23>: neg %eax
112 0x00007ffff7b08c89 <+25>: mov %eax,%fs:(%rcx)
113 0x00007ffff7b08c8c <+28>: or $0xffffffffffffffff,%rax
114 0x00007ffff7b08c90 <+32>: retq
115 End of assembler dump.
116 (gdb)
117
118 (gdb) cont
119 Continuing.
120 > TESTME
121 63: SCREEN!
122
123
124 BBreakpoint 2, main () at src/dup2_example.c:68
125 68 dup2(save_stdout_fd, STDOUT_FILENO);
126 => 0x0000555555554b30 <main+310>: 8b 85 e8 fb ff ff mov -0x418(%rbp),%eax
127 0x0000555555554b36 <main+316>: be 01 00 00 00 mov $0x1,%esi
128 0x0000555555554b3b <main+321>: 89 c7 mov %eax,%edi
129 0x0000555555554b3d <main+323>: e8 1e fd ff ff callq 0x555555554860 <dup2@plt>
130 (gdb) stepi
131 0x0000555555554b36 68 dup2(save_stdout_fd, STDOUT_FILENO);
132 0x0000555555554b30 <main+310>: 8b 85 e8 fb ff ff mov -0x418(%rbp),%eax
133 => 0x0000555555554b36 <main+316>: be 01 00 00 00 mov $0x1,%esi
134 0x0000555555554b3b <main+321>: 89 c7 mov %eax,%edi
135 0x0000555555554b3d <main+323>: e8 1e fd ff ff callq 0x555555554860 <dup2@plt>

```

```

136 (gdb)
137 0x00005555555554b3b 68      dup2(save_stdout_fd, STDOUT_FILENO);
138   0x00005555555554b30 <main+310>: 8b 85 e8 fb ff ff  mov  -0x418(%rbp),%eax
139   0x00005555555554b36 <main+316>: be 01 00 00 00  mov  $0x1,%esi
140 => 0x00005555555554b3b <main+321>: 89 c7  mov  %eax,%edi
141   0x00005555555554b3d <main+323>: e8 1e fd ff ff  callq 0x555555554860 <dup2@plt>
142 (gdb)
143 0x00005555555554b3d 68      dup2(save_stdout_fd, STDOUT_FILENO);
144   0x00005555555554b30 <main+310>: 8b 85 e8 fb ff ff  mov  -0x418(%rbp),%eax
145   0x00005555555554b36 <main+316>: be 01 00 00 00  mov  $0x1,%esi
146   0x00005555555554b3b <main+321>: 89 c7  mov  %eax,%edi
147 => 0x00005555555554b3d <main+323>: e8 1e fd ff ff  callq 0x555555554860 <dup2@plt>
148 (gdb)
149 0x00005555555554860 in dup2@plt ()
150 => 0x00005555555554860 <dup2@plt+0>: ff 25 ca 07 20 00  jmpq  *0x2007ca(%rip)          # 0x555555755030
151 (gdb) x 0x555555755030
152 0x555555755030: 0xf7b08c70
153 (gdb) disas 0x00007ffff7b08c70
154 Dump of assembler code for function dup2:
155   0x00007ffff7b08c70 <+0>: mov  $0x21,%eax
156   0x00007ffff7b08c75 <+5>: syscall
157   0x00007ffff7b08c77 <+7>: cmp  $0xffffffffffffff01,%rax
158   0x00007ffff7b08c7d <+13>: jae  0x7ffff7b08c80 <dup2+16>
159   0x00007ffff7b08c7f <+15>: retq
160   0x00007ffff7b08c80 <+16>: mov  0x2c9179(%rip),%rcx      # 0x7ffff7dd1e00
161   0x00007ffff7b08c87 <+23>: neg  %eax
162   0x00007ffff7b08c89 <+25>: mov  %eax,%fs:(%rcx)
163   0x00007ffff7b08c8c <+28>: or   $0xffffffffffffff,%rax
164   0x00007ffff7b08c90 <+32>: retq
165 End of assembler dump.
166 (gdb) stepi
167
168 Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
169 => 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00  mov  $0x21,%eax
170 (gdb)
171 0x00007ffff7b08c75 in dup2 () from /usr/lib/libc.so.6
172 => 0x00007ffff7b08c75 <dup2+5>: 0f 05  syscall
173 (gdb) cont
174 Continuing.
175 71: FINALLY: TESTME
176
177 [Inferior 1 (process 818) exited normally]
178 (gdb)
179
180

```

```
181
182
183
184 => 0x00007ffff7b08c70 <+0>: mov    $0x21,%eax
185 # 33  common dup2          sys_dup2
186 https://elixir.bootlin.com/linux/v4.14.6/source/arch/x86/entry/syscalls/syscall\_64.tbl
187
```