```
gdb run - ARCH


echo 0 | sudo tee /proc/sys/kernel/randomize_va_space



student@arch-small CS460_Code_Examples]$ gdb ./bin/dup2_example
GNU gdb (GDB) 8.0.1
...
Reading symbols from ./bin/dup2_example...done.
(gdb) break dup2
Breakpoint 1 at 0x860
(gdb) break 42
Breakpoint 2 at 0xa45: file src/dup2_example.c, line 42.
(gdb) break 68
Breakpoint 3 at 0xb30: file src/dup2_example.c, line 68.
(gdb) set disassemble-next-line on
(gdb) run
Starting program: /home/student/git/cs460_WithWorkspace/CS460_Code_Examples/bin/dup2_example
(gdb) break 42
Breakpoint 1 at 0xa45: file src/dup2_example.c, line 42.
(gdb) break 68
Breakpoint 2 at 0xb30: file src/dup2_example.c, line 68.
(gdb) break dup2
Breakpoint 3 at 0x860
(gdb) set disassemble-next-line on
(gdb) run
Starting program: /home/student/git/cs460_WithWorkspace/CS460_Code_Examples/bin/dup2_example

Breakpoint 1, main () at src/dup2_example.c:42
42      dup2(fd, STDOUT_FILENO);
=> 0x0000555555554a45 <main+75>:    8b 85 ec fb ff ff   mov    -0x414(%rbp),%eax
   0x0000555555554a4b <main+81>:    be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554a50 <main+86>:    89 c7   mov    %eax,%edi
   0x0000555555554a52 <main+88>:    e8 09 fe ff ff  callq  0x555555554860 <dup2@plt>
(gdb) stepi
0x0000555555554a4b  42      dup2(fd, STDOUT_FILENO);
   0x0000555555554a45 <main+75>:    8b 85 ec fb ff ff   mov    -0x414(%rbp),%eax
=> 0x0000555555554a4b <main+81>:    be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554a50 <main+86>:    89 c7   mov    %eax,%edi
   0x0000555555554a52 <main+88>:    e8 09 fe ff ff  callq  0x555555554860 <dup2@plt>
(gdb)
0x0000555555554a50  42      dup2(fd, STDOUT_FILENO);
   0x0000555555554a45 <main+75>:    8b 85 ec fb ff ff   mov    -0x414(%rbp),%eax
```

```
   0x0000555555554a4b <main+81>:    be 01 00 00 00  mov    $0x1,%esi
=> 0x0000555555554a50 <main+86>:    89 c7   mov    %eax,%edi
   0x0000555555554a52 <main+88>:    e8 09 fe ff ff  callq  0x555555554860 <dup2@plt>
(gdb)
0x0000555555554a52  42      dup2(fd, STDOUT_FILENO);
   0x0000555555554a45 <main+75>:    8b 85 ec fb ff ff   mov    -0x414(%rbp),%eax
   0x0000555555554a4b <main+81>:    be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554a50 <main+86>:    89 c7   mov    %eax,%edi
=> 0x0000555555554a52 <main+88>:    e8 09 fe ff ff  callq  0x555555554860 <dup2@plt>
(gdb) stepi
0x0000555555554860 in dup2@plt ()
=> 0x0000555555554860 <dup2@plt+0>: ff 25 ca 07 20 00   jmpq   *0x2007ca(%rip)        # 0x555555755030
(gdb) x 0x555555755030
0x555555755030: 0x55554866
(gdb) disas 0x55554866
No function contains specified address.
(gdb) disas 0x0000555555554866
Dump of assembler code for function dup2@plt:
=> 0x0000555555554860 <+0>: jmpq   *0x2007ca(%rip)        # 0x555555755030
   0x0000555555554866 <+6>: pushq  $0x3
   0x000055555555486b <+11>:    jmpq   0x555555554820
End of assembler dump.
(gdb)


(gdb) stepi
0x0000555555554866 in dup2@plt ()
=> 0x0000555555554866 <dup2@plt+6>: 68 03 00 00 00  pushq  $0x3
(gdb)



((gdb) stepi
0x0000555555554866 in dup2@plt ()
=> 0x0000555555554866 <dup2@plt+6>: 68 03 00 00 00  pushq  $0x3
(gdb)
0x000055555555486b in dup2@plt ()
=> 0x000055555555486b <dup2@plt+11>:    e9 b0 ff ff ff  jmpq   0x555555554820
(gdb)
0x0000555555554820 in ?? ()
=> 0x0000555555554820:  ff 35 e2 07 20 00   pushq  0x2007e2(%rip)        # 0x555555755008
(gdb)
0x0000555555554826 in ?? ()
=> 0x0000555555554826:  ff 25 e4 07 20 00   jmpq   *0x2007e4(%rip)        # 0x555555755010
(gdb)
```

```
0x00007ffff7dede10 in _dl_runtime_resolve_xsave () from /lib64/ld-linux-x86-64.so.2
=> 0x00007ffff7dede10 <_dl_runtime_resolve_xsave+0>:    53  push   %rbx
(gdb) cont
Continuing.

Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
=> 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00  mov    $0x21,%eax
(gdb)


Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
=> 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00  mov    $0x21,%eax
(gdb) disas $pc
Dump of assembler code for function dup2:
=> 0x00007ffff7b08c70 <+0>: mov    $0x21,%eax
   0x00007ffff7b08c75 <+5>: syscall
   0x00007ffff7b08c77 <+7>: cmp    $0xfffffffffffff001,%rax
   0x00007ffff7b08c7d <+13>:    jae    0x7ffff7b08c80 <dup2+16>
   0x00007ffff7b08c7f <+15>:    retq
   0x00007ffff7b08c80 <+16>:    mov    0x2c9179(%rip),%rcx        # 0x7ffff7dd1e00
   0x00007ffff7b08c87 <+23>:    neg    %eax
   0x00007ffff7b08c89 <+25>:    mov    %eax,%fs:(%rcx)
   0x00007ffff7b08c8c <+28>:    or     $0xffffffffffffffff,%rax
   0x00007ffff7b08c90 <+32>:    retq
End of assembler dump.
(gdb)

(gdb) cont
Continuing.
> TESTME
63: SCREEN!


BBreakpoint 2, main () at src/dup2_example.c:68
68      dup2(save_stdout_fd, STDOUT_FILENO);
=> 0x0000555555554b30 <main+310>:   8b 85 e8 fb ff ff   mov    -0x418(%rbp),%eax
   0x0000555555554b36 <main+316>:   be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554b3b <main+321>:   89 c7   mov    %eax,%edi
   0x0000555555554b3d <main+323>:   e8 1e fd ff ff  callq  0x555555554860 <dup2@plt>
(gdb) stepi
0x0000555555554b36  68      dup2(save_stdout_fd, STDOUT_FILENO);
   0x0000555555554b30 <main+310>:   8b 85 e8 fb ff ff   mov    -0x418(%rbp),%eax
=> 0x0000555555554b36 <main+316>:   be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554b3b <main+321>:   89 c7   mov    %eax,%edi
   0x0000555555554b3d <main+323>:   e8 1e fd ff ff  callq  0x555555554860 <dup2@plt>
```

```
(gdb)
0x0000555555554b3b  68      dup2(save_stdout_fd, STDOUT_FILENO);
   0x0000555555554b30 <main+310>:   8b 85 e8 fb ff ff   mov    -0x418(%rbp),%eax
   0x0000555555554b36 <main+316>:   be 01 00 00 00  mov    $0x1,%esi
=> 0x0000555555554b3b <main+321>:   89 c7   mov    %eax,%edi
   0x0000555555554b3d <main+323>:   e8 1e fd ff ff  callq  0x555555554860 <dup2@plt>
(gdb)
0x0000555555554b3d  68      dup2(save_stdout_fd, STDOUT_FILENO);
   0x0000555555554b30 <main+310>:   8b 85 e8 fb ff ff   mov    -0x418(%rbp),%eax
   0x0000555555554b36 <main+316>:   be 01 00 00 00  mov    $0x1,%esi
   0x0000555555554b3b <main+321>:   89 c7   mov    %eax,%edi
=> 0x0000555555554b3d <main+323>:   e8 1e fd ff ff  callq  0x555555554860 <dup2@plt>
(gdb)
0x0000555555554860 in dup2@plt ()
=> 0x0000555555554860 <dup2@plt+0>: ff 25 ca 07 20 00   jmpq   *0x2007ca(%rip)        # 0x555555755030
(gdb) x 0x555555755030
0x555555755030: 0xf7b08c70
(gdb) disas 0x00007ffff7b08c70
Dump of assembler code for function dup2:
   0x00007ffff7b08c70 <+0>: mov    $0x21,%eax
   0x00007ffff7b08c75 <+5>: syscall
   0x00007ffff7b08c77 <+7>: cmp    $0xfffffffffffff001,%rax
   0x00007ffff7b08c7d <+13>:    jae    0x7ffff7b08c80 <dup2+16>
   0x00007ffff7b08c7f <+15>:    retq
   0x00007ffff7b08c80 <+16>:    mov    0x2c9179(%rip),%rcx        # 0x7ffff7dd1e00
   0x00007ffff7b08c87 <+23>:    neg    %eax
   0x00007ffff7b08c89 <+25>:    mov    %eax,%fs:(%rcx)
   0x00007ffff7b08c8c <+28>:    or     $0xffffffffffffffff,%rax
   0x00007ffff7b08c90 <+32>:    retq
End of assembler dump.
(gdb) stepi

Breakpoint 3, 0x00007ffff7b08c70 in dup2 () from /usr/lib/libc.so.6
=> 0x00007ffff7b08c70 <dup2+0>: b8 21 00 00 00  mov    $0x21,%eax
(gdb)
0x00007ffff7b08c75 in dup2 () from /usr/lib/libc.so.6
=> 0x00007ffff7b08c75 <dup2+5>: 0f 05   syscall
(gdb) cont
Continuing.
71: FINALLY: TESTME

[Inferior 1 (process 818) exited normally]
(gdb)
```

```
=> 0x00007ffff7b08c70 <+0>: mov    $0x21,%eax
# 33    common  dup2            sys_dup2
https://elixir.bootlin.com/linux/v4.14.6/source/arch/x86/entry/syscalls/syscall_64.tbl
```