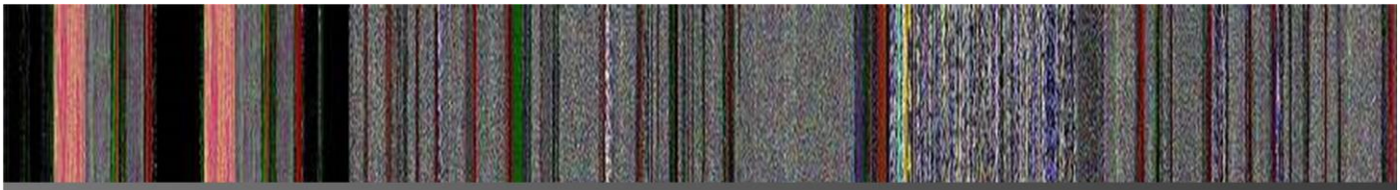


Defect

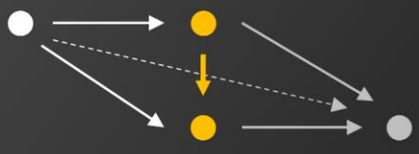
Detect

Linux API

for Software Diagnostics

Accelerated

With Category Theory in View



Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

OpenTask books and magazines are available through booksellers and distributors worldwide. For further information or comments, send requests to press@opentask.com.

A CIP catalog record for this book is available from the British Library.

ISBN-l3: 978-1-912636-62-4 (Paperback)

Revision 1.00 (June 2023)

Contents

Exercise L1 (GDB)

Goal: Explore import/export information and calls to shared libraries.

ADDR Patterns: Call Path.

1. Disassemble the *execve@plt* function from the bash executable in the x64 directory:

```
~/LAPI/x64$ objdump -d bash | grep -A 4 "<execve@plt>:"
000000000002d5e0 <execve@plt>:
   2d5e0:       ff 25 0a 7d 0e 00       jmpq   *0xe7d0a(%rip)        # 1152f0 <execve@GLIBC_2.2.5>
   2d5e6:       68 5b 00 00 00          pushq  $0x5b
   2d5eb:       e9 30 fa ff ff          jmpq   2d020 <endgrent@plt-0x10>
```

2. Dump all ELF info from the *bash* executable in the x64 directory and look for the **1152f0** entry in the *.rela.plt* section and the referenced 94 (0x**5e**) entry in the *.dynsym* section:

```
~/LAPI/x64$ readelf -a bash
[...]
Relocation section '.rela.plt' at offset 0x2b928 contains 218 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
[...]
000000001152f0  005e00000007 R_X86_64_JUMP_SLO 0000000000000000 execve@GLIBC_2.2.5 + 0
[...]
Symbol table '.dynsym' contains 2432 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
[...]
    94: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND execve@GLIBC_2.2.5 (2)
[...]
```

3. Dump all ELF info from the *libc.so.6* shared library in the x64 directory and look for the *execve@GLIBC* function in the *.dynsym* section:

```
~/LAPI/x64$ readelf -a libc.so.6
[...]
Symbol table '.dynsym' contains 2359 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
[...]
  1508: 00000000000c68a0    33 FUNC    WEAK   DEFAULT   13 execve@@GLIBC_2.2.5
```

4. Load a core dump *core.9* and *bash* executable from the x64 directory:

```
~/LAPI/x64$ gdb -c core.9 -se bash
GNU gdb (Debian 8.2.1-2+b3) 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 "x86_64-linux-gnu".
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 bash...(no debugging symbols found)...done.

warning: core file may not match specified executable file.
[New LWP 9]
Core was generated by `-bash'.
#0  0x00007f3e9f7492d7 in __GI___waitpid (pid=-1, stat_loc=0x7ffcbd661ad0, options=10) at
../sysdeps/unix/sysv/linux/waitpid.c:30
30      ../sysdeps/unix/sysv/linux/waitpid.c: No such file or directory.
```

5. Set logging to a file in case of lengthy output from some commands:

```
(gdb) set logging on L1.log
Copying output to L1.log.
```

6. Disassemble the *shell_execve* function and find the call to the *open@plt* function:

```
(gdb) disassemble shell_execve
Dump of assembler code for function shell_execve:
   0x000055e16508f7a0 <+0>:     push   %r15
   0x000055e16508f7a2 <+2>:     push   %r14
   0x000055e16508f7a4 <+4>:     mov    %rdx,%r14
   0x000055e16508f7a7 <+7>:     push   %r13
   0x000055e16508f7a9 <+9>:     mov    %rsi,%r13
   0x000055e16508f7ac <+12>:    push   %r12
   0x000055e16508f7ae <+14>:    push   %rbp
   0x000055e16508f7af <+15>:    push   %rbx
   0x000055e16508f7b0 <+16>:    mov    %rdi,%rbx
   0x000055e16508f7b3 <+19>:    sub    $0xa8,%rsp
   0x000055e16508f7ba <+26>:    mov    %fs:0x28,%rax
   0x000055e16508f7c3 <+35>:    mov    %rax,0x98(%rsp)
   0x000055e16508f7cb <+43>:    xor    %eax,%eax
   0x000055e16508f7cd <+45>:    callq  0x55e1650785e0 <execve@plt>
   0x000055e16508f7d2 <+50>:    callq  0x55e165078120 <__errno_location@plt>
   0x000055e16508f7d7 <+55>:    mov    %rax,%r12
   0x000055e16508f7da <+58>:    mov    (%rax),%ebp
   0x000055e16508f7dc <+60>:    mov    0xdc2a6(%rip),%eax        # 0x55e16516ba88
<terminating_signal>
   0x000055e16508f7e2 <+66>:    test   %eax,%eax
   0x000055e16508f7e4 <+68>:    jne    0x55e16508f880 <shell_execve+224>
   0x000055e16508f7ea <+74>:    cmp    $0x8,%ebp
   0x000055e16508f7ed <+77>:    je     0x55e16508f894 <shell_execve+244>
   0x000055e16508f7f3 <+83>:    xor    %eax,%eax
   0x000055e16508f7f5 <+85>:    cmp    $0x2,%ebp
   0x000055e16508f7f8 <+88>:    mov    %rbx,%rdi
   0x000055e16508f7fb <+91>:    sete   %al
   0x000055e16508f7fe <+94>:    add    $0x7e,%eax
   0x000055e16508f801 <+97>:    mov    %eax,0xde321(%rip)        # 0x55e16516db28
<last_command_exit_value>
   0x000055e16508f807 <+103>:   callq  0x55e1650891a0 <file_isdir>
   0x000055e16508f80c <+108>:   test   %eax,%eax
   0x000055e16508f80e <+110>:   jne    0x55e16508fa58 <shell_execve+696>
   0x000055e16508f814 <+116>:   mov    %rbx,%rdi
   0x000055e16508f817 <+119>:   callq  0x55e1650d3970 <executable_file>
   0x000055e16508f81c <+124>:   test   %eax,%eax
   0x000055e16508f81e <+126>:   je     0x55e16508f841 <shell_execve+161>
   0x000055e16508f820 <+128>:   cmp    $0x7,%ebp
   0x000055e16508f823 <+131>:   je     0x55e16508f841 <shell_execve+161>
```

```
   0x000055e16508f825 <+133>:   cmp    $0xc,%ebp
   0x000055e16508f828 <+136>:   je     0x55e16508f841 <shell_execve+161>
   0x000055e16508f82a <+138>:   xor    %esi,%esi
   0x000055e16508f82c <+140>:   mov    %rbx,%rdi
   0x000055e16508f82f <+143>:   xor    %eax,%eax
   0x000055e16508f831 <+145>:   callq  0x55e165078aa0 <open@plt>
   0x000055e16508f836 <+150>:   mov    %eax,%r13d
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
```

7. Follow the call path and indirect jump to see the real call from the *libc.so.6* library:

```
(gdb) disassemble 0x55e165078aa0
Dump of assembler code for function open@plt:
   0x000055e165078aa0 <+0>:     jmpq   *0xe7aaa(%rip)        # 0x55e165160550 <open@got.plt>
   0x000055e165078aa6 <+6>:     pushq  $0xa7
   0x000055e165078aab <+11>:    jmpq   0x55e165078020
End of assembler dump.

(gdb) x/a 0x55e165160550
0x55e165160550 <open@got.plt>:  0x7f3e9f76d010 <__libc_open64>

(gdb) info sharedlibrary
From                To                  Syms Read   Shared Object Library
0x00007f3e9f856950  0x00007f3e9f863dc8  Yes (*)     /lib/x86_64-linux-gnu/libtinfo.so.6
0x00007f3e9f844130  0x00007f3e9f844eb5  Yes         /lib/x86_64-linux-gnu/libdl.so.2
0x00007f3e9f6a5320  0x00007f3e9f7eb14b  Yes         /lib/x86_64-linux-gnu/libc.so.6
0x00007f3e9f884090  0x00007f3e9f8a1b50  Yes         /lib64/ld-linux-x86-64.so.2
0x00007f3e9f37e300  0x00007f3e9f384578  Yes         /lib/x86_64-linux-gnu/libnss_files.so.2
(*): Shared library is missing debugging information.
```

8. We can also check the section for the address **0x55e165160550**:

```
(gdb) info file
Symbols from "/home/coredump/LAPI/x64/bash".
Local core dump file:
        `/home/coredump/LAPI/x64/core.9', file type elf64-x86-64.
        0x000055e16515d000 - 0x000055e165160000 is load1
        0x000055e165160000 - 0x000055e165169000 is load2
        0x000055e165169000 - 0x000055e165173000 is load3
        0x000055e1667f5000 - 0x000055e166879000 is load4
        0x00007f3e9f388000 - 0x00007f3e9f389000 is load5
        0x00007f3e9f389000 - 0x00007f3e9f38a000 is load6
        0x00007f3e9f38a000 - 0x00007f3e9f390000 is load7
        0x00007f3e9f680000 - 0x00007f3e9f683000 is load8
        0x00007f3e9f839000 - 0x00007f3e9f83d000 is load9
        0x00007f3e9f83d000 - 0x00007f3e9f83f000 is load10
        0x00007f3e9f83f000 - 0x00007f3e9f843000 is load11
        0x00007f3e9f846000 - 0x00007f3e9f847000 is load12
        0x00007f3e9f847000 - 0x00007f3e9f848000 is load13
        0x00007f3e9f871000 - 0x00007f3e9f875000 is load14
        0x00007f3e9f875000 - 0x00007f3e9f876000 is load15
        0x00007f3e9f876000 - 0x00007f3e9f878000 is load16
        0x00007f3e9f8aa000 - 0x00007f3e9f8ab000 is load17
        0x00007f3e9f8ab000 - 0x00007f3e9f8ac000 is load18
        0x00007f3e9f8ac000 - 0x00007f3e9f8ad000 is load19
        0x00007ffcbd642000 - 0x00007ffcbd663000 is load20
        0x00007ffcbd7ea000 - 0x00007ffcbd7eb000 is load21
Local exec file:
        `/home/coredump/LAPI/x64/bash', file type elf64-x86-64.
        Entry point: 0x55e16507a630
        0x000055e16504b2a8 - 0x000055e16504b2c4 is .interp
        0x000055e16504b2c4 - 0x000055e16504b2e4 is .note.ABI-tag
        0x000055e16504b2e4 - 0x000055e16504b308 is .note.gnu.build-id
        0x000055e16504b308 - 0x000055e16504fdb0 is .gnu.hash
        0x000055e16504fdb0 - 0x000055e16505e1b0 is .dynsym
```

```
        0x000055e16505e1b0 - 0x000055e1650678d8 is .dynstr
        0x000055e1650678d8 - 0x000055e165068bd8 is .gnu.version
        0x000055e165068bd8 - 0x000055e165068ca8 is .gnu.version_r
        0x000055e165068ca8 - 0x000055e165076928 is .rela.dyn
        0x000055e165076928 - 0x000055e165077d98 is .rela.plt
        0x000055e165078000 - 0x000055e165078017 is .init
        0x000055e165078020 - 0x000055e165078dd0 is .plt
        0x000055e165078dd0 - 0x000055e165078de8 is .plt.got
        0x000055e165078df0 - 0x000055e165125781 is .text
        0x000055e165125784 - 0x000055e16512578d is .fini
        0x000055e165126000 - 0x000055e16513f930 is .rodata
        0x000055e16513f930 - 0x000055e165143df4 is .eh_frame_hdr
        0x000055e165143df8 - 0x000055e16515b730 is .eh_frame
        0x000055e16515d3f0 - 0x000055e16515d3f8 is .init_array
        0x000055e16515d3f8 - 0x000055e16515d400 is .fini_array
        0x000055e16515d400 - 0x000055e16515fcf0 is .data.rel.ro
--Type <RET> for more, q to quit, c to continue without paging--
        0x000055e16515fcf0 - 0x000055e16515fef0 is .dynamic
        0x000055e16515fef0 - 0x000055e16515fff0 is .got
        0x000055e165160000 - 0x000055e1651606e8 is .got.plt
        0x000055e165160700 - 0x000055e165168d04 is .data
        0x000055e165168d20 - 0x000055e165172998 is .bss
        0x00007f3e9f848238 - 0x00007f3e9f84825c is .note.gnu.build-id in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f848260 - 0x00007f3e9f848a78 is .gnu.hash in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f848a78 - 0x00007f3e9f84a7a0 is .dynsym in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f84a7a0 - 0x00007f3e9f84b71a is .dynstr in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f84b71a - 0x00007f3e9f84b988 is .gnu.version in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f84b988 - 0x00007f3e9f84bd34 is .gnu.version_d in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f84bd38 - 0x00007f3e9f84bda8 is .gnu.version_r in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f84bda8 - 0x00007f3e9f854d48 is .rela.dyn in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f854d48 - 0x00007f3e9f855ae0 is .rela.plt in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f856000 - 0x00007f3e9f856017 is .init in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f856020 - 0x00007f3e9f856940 is .plt in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f856940 - 0x00007f3e9f856950 is .plt.got in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f856950 - 0x00007f3e9f863dc8 is .text in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f863dc8 - 0x00007f3e9f863dd1 is .fini in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f864000 - 0x00007f3e9f86d9a5 is .rodata in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f86d9a8 - 0x00007f3e9f86e13c is .eh_frame_hdr in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f86e140 - 0x00007f3e9f8706b0 is .eh_frame in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f8718d0 - 0x00007f3e9f8718d8 is .init_array in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f8718d8 - 0x00007f3e9f8718e0 is .fini_array in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f8718e0 - 0x00007f3e9f874848 is .data.rel.ro in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f874848 - 0x00007f3e9f874a58 is .dynamic in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f874a58 - 0x00007f3e9f874ff8 is .got in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f875000 - 0x00007f3e9f8754f4 is .data in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f875500 - 0x00007f3e9f875980 is .bss in /lib/x86_64-linux-gnu/libtinfo.so.6
        0x00007f3e9f843238 - 0x00007f3e9f84325c is .note.gnu.build-id in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f84325c - 0x00007f3e9f84327c is .note.ABI-tag in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843280 - 0x00007f3e9f843348 is .gnu.hash in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843348 - 0x00007f3e9f843750 is .dynsym in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843750 - 0x00007f3e9f843989 is .dynstr in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f84398a - 0x00007f3e9f8439e0 is .gnu.version in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f8439e0 - 0x00007f3e9f843a84 is .gnu.version_d in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843a88 - 0x00007f3e9f843ae8 is .gnu.version_r in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843ae8 - 0x00007f3e9f843c80 is .rela.dyn in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f843c80 - 0x00007f3e9f843db8 is .rela.plt in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f844000 - 0x00007f3e9f844017 is .init in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f844020 - 0x00007f3e9f844100 is .plt in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f844100 - 0x00007f3e9f844128 is .plt.got in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f844130 - 0x00007f3e9f844eb5 is .text in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f844eb8 - 0x00007f3e9f844ec1 is .fini in /lib/x86_64-linux-gnu/libdl.so.2
        0x00007f3e9f845000 - 0x00007f3e9f8450a3 is .rodata in /lib/x86_64-linux-gnu/libdl.so.2
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
```

9. Load a core dump *core.19649* and *bash* executable from the A64 directory:

```
~/LAPI/x64$ cd ../A64

~/LAPI/A64$ gdb-multiarch -c core.19649 -se bash
GNU gdb (Debian 8.2.1-2+b3) 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 "x86_64-linux-gnu".
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 bash...(no debugging symbols found)...done.

warning: core file may not match specified executable file.
[New LWP 19649]

warning: Could not load shared library symbols for 3 libraries, e.g. /lib/aarch64-linux-
gnu/libtinfo.so.6.
Use the "info sharedlibrary" command to see the complete listing.
Do you need "set solib-search-path" or "set sysroot"?
Core was generated by `-bash'.
#0  0x0000ffffbafa6734 in ?? ()
```

```
(gdb) set solib-search-path .
Reading symbols from /home/coredump/LAPI/A64/libtinfo.so.6...(no debugging symbols found)...done.
Reading symbols from /home/coredump/LAPI/A64/libc.so.6...(no debugging symbols found)...done.
Reading symbols from /home/coredump/LAPI/A64/ld-linux-aarch64.so.1...(no debugging symbols found)...done.
```

10. Set logging to a file in case of lengthy output from some commands:

```
(gdb) set logging on L1.log
Copying output to L1.log.
```

11. Disassemble the *shell_execve* function and find the call to the *open@plt* function:

```
(gdb) disassemble shell_execve
Dump of assembler code for function shell_execve:
   0x0000aaaabb6f7144 <+0>:     stp     x29, x30, [sp, #-224]!
   0x0000aaaabb6f7148 <+4>:     adrp    x3, 0xaaaabb800000
   0x0000aaaabb6f714c <+8>:     mov     x29, sp
   0x0000aaaabb6f7150 <+12>:    ldr     x3, [x3, #1192]
   0x0000aaaabb6f7154 <+16>:    stp     x19, x20, [sp, #16]
   0x0000aaaabb6f7158 <+20>:    mov     x19, x0
   0x0000aaaabb6f715c <+24>:    stp     x21, x22, [sp, #32]
   0x0000aaaabb6f7160 <+28>:    mov     x22, x1
   0x0000aaaabb6f7164 <+32>:    stp     x23, x24, [sp, #48]
   0x0000aaaabb6f7168 <+36>:    mov     x23, x2
   0x0000aaaabb6f716c <+40>:    stp     x25, x26, [sp, #64]
   0x0000aaaabb6f7170 <+44>:    ldr     x4, [x3]
   0x0000aaaabb6f7174 <+48>:    str     x4, [sp, #216]
   0x0000aaaabb6f7178 <+52>:    mov     x4, #0x0                        // #0
   0x0000aaaabb6f717c <+56>:    bl      0xaaaabb6d23e0 <execve@plt>
   0x0000aaaabb6f7180 <+60>:    bl      0xaaaabb6d2740 <__errno_location@plt>
   0x0000aaaabb6f7184 <+64>:    mov     x20, x0
   0x0000aaaabb6f7188 <+68>:    adrp    x3, 0xaaaabb800000
   0x0000aaaabb6f718c <+72>:    ldr     x0, [x3, #2616]
   0x0000aaaabb6f7190 <+76>:    ldr     w1, [x0]
   0x0000aaaabb6f7194 <+80>:    cbnz    w1, 0xaaaabb6f72bc <shell_execve+376>
```

```
   0x0000aaaabb6f7198 <+84>:    ldr     w21, [x20]
   0x0000aaaabb6f719c <+88>:    cmp     w21, #0x8
   0x0000aaaabb6f71a0 <+92>:    b.eq    0xaaaabb6f73c4 <shell_execve+640>  // b.none
   0x0000aaaabb6f71a4 <+96>:    adrp    x23, 0xaaaabb800000
   0x0000aaaabb6f71a8 <+100>:   cmp     w21, #0x2
   0x0000aaaabb6f71ac <+104>:   cset    w2, eq  // eq = none
   0x0000aaaabb6f71b0 <+108>:   add     x24, sp, #0x58
   0x0000aaaabb6f71b4 <+112>:   ldr     x3, [x23, #3744]
   0x0000aaaabb6f71b8 <+116>:   add     w2, w2, #0x7e
   0x0000aaaabb6f71bc <+120>:   mov     x1, x24
   0x0000aaaabb6f71c0 <+124>:   mov     x0, x19
   0x0000aaaabb6f71c4 <+128>:   str     w2, [x3]
   0x0000aaaabb6f71c8 <+132>:   bl      0xaaaabb6d2180 <stat@plt>
   0x0000aaaabb6f71cc <+136>:   cbnz    w0, 0xaaaabb6f71e0 <shell_execve+156>
   0x0000aaaabb6f71d0 <+140>:   ldr     w0, [sp, #104]
   0x0000aaaabb6f71d4 <+144>:   and     w0, w0, #0xf000
   0x0000aaaabb6f71d8 <+148>:   cmp     w0, #0x4, lsl #12
   0x0000aaaabb6f71dc <+152>:   b.eq    0xaaaabb6f7288 <shell_execve+324>  // b.none
   0x0000aaaabb6f71e0 <+156>:   mov     x0, x19
   0x0000aaaabb6f71e4 <+160>:   bl      0xaaaabb742530 <file_status>
   0x0000aaaabb6f71e8 <+164>:   tbnz    w0, #4, 0xaaaabb6f727c <shell_execve+312>
   0x0000aaaabb6f71ec <+168>:   mov     w1, #0x12                       // #18
   0x0000aaaabb6f71f0 <+172>:   and     w22, w0, w1
--Type <RET> for more, q to quit, c to continue without paging--
   0x0000aaaabb6f71f4 <+176>:   cmp     w22, #0x2
   0x0000aaaabb6f71f8 <+180>:   b.ne    0xaaaabb6f721c <shell_execve+216>  // b.any
   0x0000aaaabb6f71fc <+184>:   cmp     w21, #0x7
   0x0000aaaabb6f7200 <+188>:   ccmp    w21, #0xc, #0x4, ne  // ne = any
   0x0000aaaabb6f7204 <+192>:   b.eq    0xaaaabb6f721c <shell_execve+216>  // b.none
   0x0000aaaabb6f7208 <+196>:   mov     x0, x19
   0x0000aaaabb6f720c <+200>:   mov     w1, #0x0                        // #0
   0x0000aaaabb6f7210 <+204>:   bl      0xaaaabb6d1ec0 <open@plt>
   0x0000aaaabb6f7214 <+208>:   mov     w25, w0
   0x0000aaaabb6f7218 <+212>:   tbz     w0, #31, 0xaaaabb6f72d0 <shell_execve+396>
   0x0000aaaabb6f721c <+216>:   str     w21, [x20]
   0x0000aaaabb6f7220 <+220>:   mov     w0, w21
   0x0000aaaabb6f7224 <+224>:   bl      0xaaaabb6d2110 <strerror@plt>
   0x0000aaaabb6f7228 <+228>:   mov     x2, x0
   0x0000aaaabb6f722c <+232>:   mov     x1, x19
   0x0000aaaabb6f7230 <+236>:   adrp    x0, 0xaaaabb7c4000
   0x0000aaaabb6f7234 <+240>:   add     x0, x0, #0xbd8
   0x0000aaaabb6f7238 <+244>:   bl      0xaaaabb706674 <report_error>
   0x0000aaaabb6f723c <+248>:   ldr     x23, [x23, #3744]
   0x0000aaaabb6f7240 <+252>:   ldr     w25, [x23]
   0x0000aaaabb6f7244 <+256>:   adrp    x0, 0xaaaabb800000
   0x0000aaaabb6f7248 <+260>:   ldr     x0, [x0, #1192]
   0x0000aaaabb6f724c <+264>:   ldr     x2, [sp, #216]
   0x0000aaaabb6f7250 <+268>:   ldr     x1, [x0]
   0x0000aaaabb6f7254 <+272>:   subs    x2, x2, x1
   0x0000aaaabb6f7258 <+276>:   mov     x1, #0x0                        // #0
   0x0000aaaabb6f725c <+280>:   b.ne    0xaaaabb6f77ec <shell_execve+1704>  // b.any
   0x0000aaaabb6f7260 <+284>:   mov     w0, w25
   0x0000aaaabb6f7264 <+288>:   ldp     x19, x20, [sp, #16]
   0x0000aaaabb6f7268 <+292>:   ldp     x21, x22, [sp, #32]
   0x0000aaaabb6f726c <+296>:   ldp     x23, x24, [sp, #48]
   0x0000aaaabb6f7270 <+300>:   ldp     x25, x26, [sp, #64]
   0x0000aaaabb6f7274 <+304>:   ldp     x29, x30, [sp], #224
   0x0000aaaabb6f7278 <+308>:   ret
   0x0000aaaabb6f727c <+312>:   mov     w1, #0x15                       // #21
   0x0000aaaabb6f7280 <+316>:   str     w1, [x20]
```

```
   0x0000aaaabb6f7284 <+320>:   b       0xaaaabb6f71ec <shell_execve+168>
   0x0000aaaabb6f7288 <+324>:   adrp    x1, 0xaaaabb7c4000
   0x0000aaaabb6f728c <+328>:   add     x1, x1, #0xbd8
   0x0000aaaabb6f7290 <+332>:   mov     w2, #0x5                        // #5
   0x0000aaaabb6f7294 <+336>:   mov     x0, #0x0                        // #0
   0x0000aaaabb6f7298 <+340>:   bl      0xaaaabb6d2630 <dcgettext@plt>
   0x0000aaaabb6f729c <+344>:   mov     x20, x0
   0x0000aaaabb6f72a0 <+348>:   mov     w0, #0x15                       // #21
   0x0000aaaabb6f72a4 <+352>:   bl      0xaaaabb6d2110 <strerror@plt>
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
```

12. Follow the call path to see the real branch and link to the *libc.so.6* library:

```
(gdb) disassemble 0xaaaabb6d1ec0
Dump of assembler code for function open@plt:
   0x0000aaaabb6d1ec0 <+0>:     adrp    x16, 0xaaaabb7ff000
   0x0000aaaabb6d1ec4 <+4>:     ldr     x17, [x16, #1464]
   0x0000aaaabb6d1ec8 <+8>:     add     x16, x16, #0x5b8
   0x0000aaaabb6d1ecc <+12>:    br      x17
End of assembler dump.

(gdb) x/a 0xaaaabb7ff000+1464
0xaaaabb7ff5b8 <open@got.plt>:  0xffffbafc7810 <open64>

(gdb) info sharedlibrary
From                To                  Syms Read   Shared Object Library
0x0000ffffbb0ad860  0x0000ffffbb0bcb88  Yes (*)     /home/coredump/LAPI/A64/libtinfo.so.6
0x0000ffffbaf17040  0x0000ffffbb023f20  Yes (*)     /home/coredump/LAPI/A64/libc.so.6
0x0000ffffbb0eec40  0x0000ffffbb10d064  Yes (*)     /home/coredump/LAPI/A64/ld-linux-
aarch64.so.1
(*): Shared library is missing debugging information.
```

13. We can also check the section for the address **0xaaaabb7ff000+1464 (0xaaaabb7ff5b8)**:

```
(gdb) info file
Symbols from "/home/coredump/LAPI/A64/bash".
Local core dump file:
        `/home/coredump/LAPI/A64/core.19649', file type elf64-littleaarch64.
        0x0000aaaabb6a0000 - 0x0000aaaabb7ed000 is load1
        0x0000aaaabb7fc000 - 0x0000aaaabb801000 is load2
        0x0000aaaabb801000 - 0x0000aaaabb80a000 is load3
        0x0000aaaabb80a000 - 0x0000aaaabb815000 is load4
        0x0000aaaae4664000 - 0x0000aaaae4815000 is load5
        0x0000ffffbaef0000 - 0x0000ffffbb079000 is load6
        0x0000ffffbb088000 - 0x0000ffffbb08c000 is load7
        0x0000ffffbb08c000 - 0x0000ffffbb08e000 is load8
        0x0000ffffbb08e000 - 0x0000ffffbb09a000 is load9
        0x0000ffffbb0a0000 - 0x0000ffffbb0cc000 is load10
        0x0000ffffbb0db000 - 0x0000ffffbb0df000 is load11
        0x0000ffffbb0df000 - 0x0000ffffbb0e0000 is load12
        0x0000ffffbb0ed000 - 0x0000ffffbb118000 is load13
        0x0000ffffbb119000 - 0x0000ffffbb11b000 is load14
        0x0000ffffbb122000 - 0x0000ffffbb124000 is load15
        0x0000ffffbb126000 - 0x0000ffffbb127000 is load16
        0x0000ffffbb127000 - 0x0000ffffbb129000 is load17
        0x0000ffffbb129000 - 0x0000ffffbb12b000 is load18
        0x0000ffffc5fb8000 - 0x0000ffffc5fd9000 is load19
Local exec file:
```

```
        `/home/coredump/LAPI/A64/bash', file type elf64-littleaarch64.
        Entry point: 0xaaaabb6d4440
        0x0000aaaabb6a0238 - 0x0000aaaabb6a0253 is .interp
        0x0000aaaabb6a0254 - 0x0000aaaabb6a0278 is .note.gnu.build-id
        0x0000aaaabb6a0278 - 0x0000aaaabb6a0298 is .note.ABI-tag
        0x0000aaaabb6a0298 - 0x0000aaaabb6a4e54 is .gnu.hash
        0x0000aaaabb6a4e58 - 0x0000aaaabb6b3a50 is .dynsym
        0x0000aaaabb6b3a50 - 0x0000aaaabb6bd6f7 is .dynstr
        0x0000aaaabb6bd6f8 - 0x0000aaaabb6beaa2 is .gnu.version
        0x0000aaaabb6beaa8 - 0x0000aaaabb6beb38 is .gnu.version_r
        0x0000aaaabb6beb38 - 0x0000aaaabb6d0538 is .rela.dyn
        0x0000aaaabb6d0538 - 0x0000aaaabb6d1a50 is .rela.plt
        0x0000aaaabb6d1a50 - 0x0000aaaabb6d1a68 is .init
        0x0000aaaabb6d1a70 - 0x0000aaaabb6d28a0 is .plt
        0x0000aaaabb6d28c0 - 0x0000aaaabb7af8b0 is .text
        0x0000aaaabb7af8b0 - 0x0000aaaabb7af8c4 is .fini
        0x0000aaaabb7af8c8 - 0x0000aaaabb7c8f24 is .rodata
        0x0000aaaabb7c8f24 - 0x0000aaaabb7cd4f0 is .eh_frame_hdr
        0x0000aaaabb7cd4f0 - 0x0000aaaabb7ec480 is .eh_frame
        0x0000aaaabb7fc818 - 0x0000aaaabb7fc820 is .init_array
        0x0000aaaabb7fc820 - 0x0000aaaabb7fc828 is .fini_array
        0x0000aaaabb7fc828 - 0x0000aaaabb7ff178 is .data.rel.ro
        0x0000aaaabb7ff178 - 0x0000aaaabb7ff388 is .dynamic
        0x0000aaaabb7ff388 - 0x0000aaaabb801000 is .got
        0x0000aaaabb801000 - 0x0000aaaabb809280 is .data
--Type <RET> for more, q to quit, c to continue without paging--q
Quit
```

Note: We see that for ARM64 implementation it is .GOT (Global Offset Table) section.