Using ltrace

Saturday, 14 March 2020 12:06 PM

Source code

```c
#include <stdio.h>
#define SMALL_SIZE 32

int main(void)
{
    char name[SMALL_SIZE];
    char color[SMALL_SIZE];

    printf("%15s", "");
    printf("What is your name? ");
    scanf("%s", name);

    printf("%15s", "");
    printf("What is your favorite color? ");
    scanf("%s", color);

    printf("%15s", "");
    printf("%s's favorite color is %s !!\n", name, color);

    return(0);
}
```

s

Tracing libc function usage

```
tao@unixuser-vm:~/cprog/chap4$ ltrace ./ex6
printf("%15s", "")                                                              = 15
printf("What is your name? ")                                                   = 19
__isoc99_scanf(0x4006be, 0x7fffffffe450, 0, 0              What is your name? tom
)                                                                  = 1
printf("%15s", "")                                                              = 15
printf("What is your favorite color? ")                                         = 29
__isoc99_scanf(0x4006be, 0x7fffffffe430, 0, 0              What is your favorite color? red
)                                                                  = 1
printf("%15s", "")                                                              = 15
printf("%s's favorite color is %s !!\n", "tom", "red"                tom's favorite color is red !!
)                                                                 = 31
+++ exited (status 0) +++
```

Determine dynamic loadable libraries

```
tao@unixuser-vm:~/cprog/chap4$ ldd ./ex6
        linux-vdso.so.1 (0x00007ffff7ffb000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ffff79e4000)
        /lib64/ld-linux-x86-64.so.2 (0x00007ffff7dd5000)
tao@unixuser-vm:~/cprog/chap4$
```

Determine the loaded function in libc

```
tao@unixuser-vm:~/cprog/chap4$ objdump -D -M intel /lib/x86_64-linux-gnu/libc.so.6 | grep __isoc99_scanf
000000000007bec0 <__isoc99_scanf@@GLIBC_2.7>:
   7bee6:       74 37                   je     7bf1f <__isoc99_scanf@@GLIBC_2.7+0x5f>
   7bf43:       75 59                   jne    7bf9e <__isoc99_scanf@@GLIBC_2.7+0xde>
   7bf59:       74 3f                   je     7bf9a <__isoc99_scanf@@GLIBC_2.7+0xda>
   7bf67:       74 08                   je     7bf71 <__isoc99_scanf@@GLIBC_2.7+0xb1>
   7bf6d:       75 07                   jne    7bf76 <__isoc99_scanf@@GLIBC_2.7+0xb6>
   7bf6f:       eb 1b                   jmp    7bf8c <__isoc99_scanf@@GLIBC_2.7+0xcc>
   7bf74:       74 16                   je     7bf8c <__isoc99_scanf@@GLIBC_2.7+0xcc>
   7bfe4:       75 3f                   jne    7c025 <__isoc99_scanf@@GLIBC_2.7+0x165>
   7bff1:       75 32                   jne    7c025 <__isoc99_scanf@@GLIBC_2.7+0x165>
   7c002:       74 07                   je     7c00b <__isoc99_scanf@@GLIBC_2.7+0x14b>
   7c007:       75 06                   jne    7c00f <__isoc99_scanf@@GLIBC_2.7+0x14f>
   7c009:       eb 1a                   jmp    7c025 <__isoc99_scanf@@GLIBC_2.7+0x165>
   7c00d:       74 16                   je     7c025 <__isoc99_scanf@@GLIBC_2.7+0x165>
   7c035:       75 09                   jne    7c040 <__isoc99_scanf@@GLIBC_2.7+0x180>
   7c052:       75 3f                   jne    7c093 <__isoc99_scanf@@GLIBC_2.7+0x1d3>
   7c05f:       75 32                   jne    7c093 <__isoc99_scanf@@GLIBC_2.7+0x1d3>
   7c070:       74 07                   je     7c079 <__isoc99_scanf@@GLIBC_2.7+0x1b9>
   7c075:       75 06                   jne    7c07d <__isoc99_scanf@@GLIBC_2.7+0x1bd>
   7c077:       eb 1a                   jmp    7c093 <__isoc99_scanf@@GLIBC_2.7+0x1d3>
   7c07b:       74 16                   je     7c093 <__isoc99_scanf@@GLIBC_2.7+0x1d3>
```