Building a Web Server

Linux Processes

Connor Nelson
Arizona State University

# read

```
int read(
    int fd,
    void *buf,
    size_t count
)
```

read() attempts to read up to count bytes from file descriptor fd into the buffer starting at buf.

# write

```
int write(
    int fd,
    void *buf,
    size_t count
)
```

write() writes up to count bytes from the buffer starting at buf to the file referred to by the file descriptor fd.

# open

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The open() system call opens the file specified by pathname. If the specified file does not exist, it may optionally (if O_CREAT is specified in flags) be created by open().

# open

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The return value of open() is a file descriptor, a small, nonnegative integer that is used in subsequent system calls (read(2), write(2), lseek(2), fcntl(2), etc.) to refer to the open file. The file descriptor returned by a successful call will be the lowest-numbered file descriptor not currently open for the process.

Linux Process

```
struct task_struct *current
```

PROCESS	
PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1
555555554000-555555555000 r--p /bin/program 555555555000-555555556000 r-xp /bin/program ... 7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6 7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6 ... 7ffffffde000-7ffffffff000 rw-p [stack]	

Linux Process

struct task_struct *current

MEMORY

```
0000555555554000   00 00 00 00 00 00 00 00 | ........
0000555555554008   00 00 00 00 00 00 00 00 | ........
0000555555554010   00 00 00 00 00 00 00 00 | ........
...                ...
0000555555555000   00 00 00 00 00 00 00 00 | ........
0000555555555008   00 00 00 00 00 00 00 00 | ........
0000555555555010   00 00 00 00 00 00 00 00 | ........
0000555555555018   00 00 00 00 00 00 00 00 | ........
...                ...
00007fffffffe000   00 00 00 00 00 00 00 00 | ........
00007fffffffe008   00 00 00 00 00 00 00 00 | ........
00007fffffffe010   00 00 00 00 00 00 00 00 | ........
```

PROCESS	
PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1
555555554000-555555555000 r--p /bin/program 555555555000-555555556000 r-xp /bin/program ... 7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6 7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6 ... 7ffffffde000-7ffffffff000 rw-p [stack]	

Linux Process

```
struct task_struct *current
```

MEMORY

```
0000555555554000   00 00 00 00 00 00 00 00 | ........
0000555555554008   00 00 00 00 00 00 00 00 | ........
0000555555554010   00 00 00 00 00 00 00 00 | ........
...                ...
0000555555555000   00 00 00 00 00 00 00 00 | ........
0000555555555008   00 00 00 00 00 00 00 00 | ........
0000555555555010   00 00 00 00 00 00 00 00 | ........
0000555555555018   00 00 00 00 00 00 00 00 | ........
...                ...
00007ffffffe000    00 00 00 00 00 00 00 00 | ........
00007ffffffe008    00 00 00 00 00 00 00 00 | ........
00007ffffffe010    00 00 00 00 00 00 00 00 | ........
...                ...
...                ...
...                ...
```

PROCESS

```
PID                          42
PPID                         1

Real      User ID            1000
Effective User ID            1000
Saved     User ID            1000

FD 0                         /dev/pts/1
FD 1                         /dev/pts/1
FD 2                         /dev/pts/1
FD 3
FD 4
...
FD 1024

555555554000-555555555000 r--p  /bin/program
555555555000-555555556000 r-xp  /bin/program
...
7ffff7da6000-7ffff7dc8000 r--p  /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp  /lib/.../libc.so.6
...
7ffffffde000-7ffffffff000 rw-p  [stack]
```

Linux Process

```
struct task_struct *current
```

MEMORY

```
0000555555554000   00 00 00 00 00 00 00 00 | ........
0000555555554008   00 00 00 00 00 00 00 00 | ........
0000555555554010   00 00 00 00 00 00 00 00 | ........
...                ...
0000555555555000   00 00 00 00 00 00 00 00 | ........
0000555555555008   00 00 00 00 00 00 00 00 | ........
0000555555555010   00 00 00 00 00 00 00 00 | ........
0000555555555018   00 00 00 00 00 00 00 00 | ........
...                ...
00007fffffffe000   00 00 00 00 00 00 00 00 | ........
00007fffffffe008   00 00 00 00 00 00 00 00 | ........
00007fffffffe010   00 00 00 00 00 00 00 00 | ........
...                ...
...                ...
...                ...
ffff800000000000   00 00 00 00 00 00 00 00 | ........
...                ...
fffffffffffffff8   00 00 00 00 00 00 00 00 | ........
```

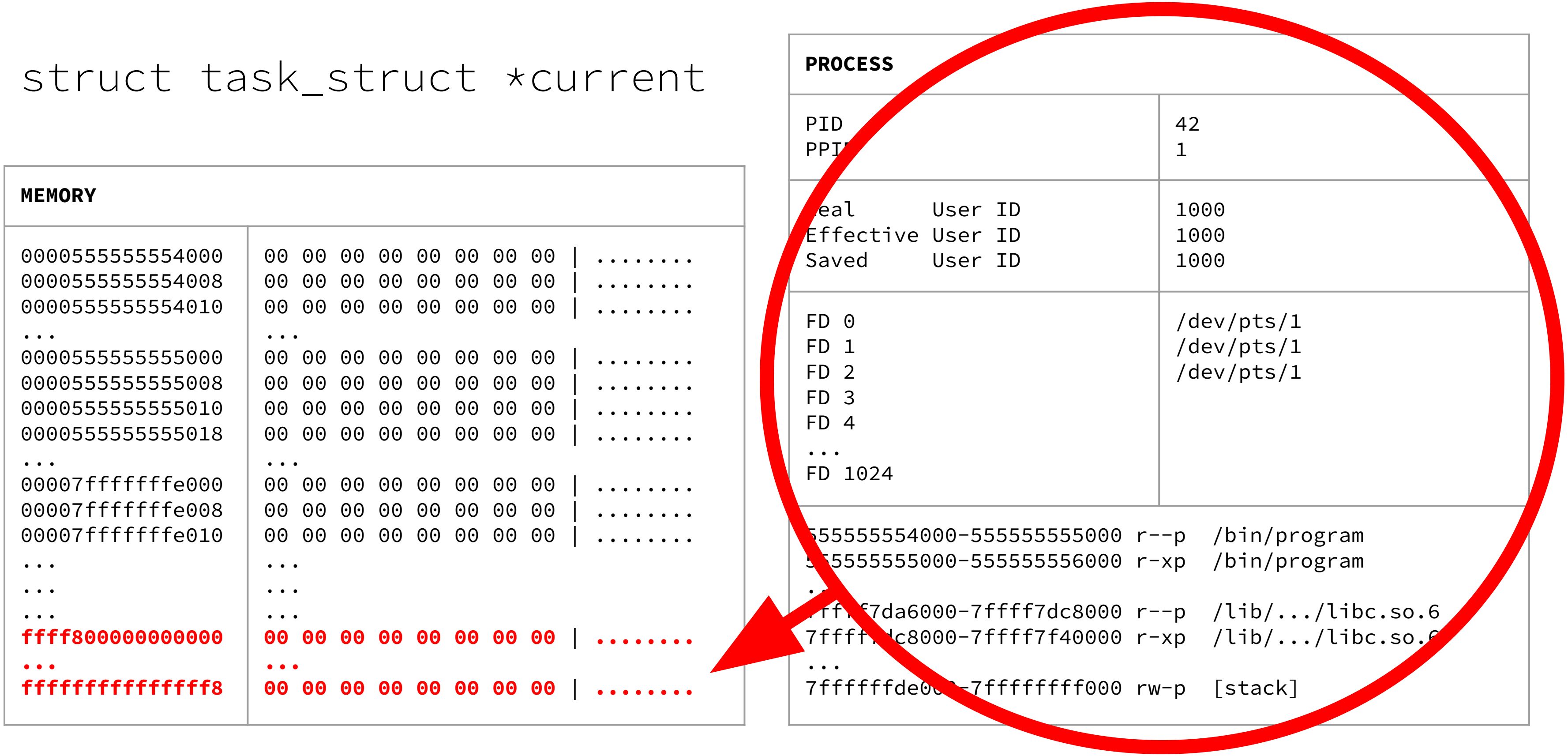
PROCESS

PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1

```
555555554000-555555555000 r--p  /bin/program
555555555000-555555556000 r-xp  /bin/program
...
7ffff7da6000-7ffff7dc8000 r--p  /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp  /lib/.../libc.so.6
...
7ffffffde000-7ffffffff000 rw-p  [stack]
```

Linux Process

```
struct task_struct *current
```



MEMORY

```
0000555555554000 | 00 00 00 00 00 00 00 00 | ........
0000555555554008 | 00 00 00 00 00 00 00 00 | ........
0000555555554010 | 00 00 00 00 00 00 00 00 | ........
...              | ...
0000555555555000 | 00 00 00 00 00 00 00 00 | ........
0000555555555008 | 00 00 00 00 00 00 00 00 | ........
0000555555555010 | 00 00 00 00 00 00 00 00 | ........
0000555555555018 | 00 00 00 00 00 00 00 00 | ........
...              | ...
00007ffffffe000  | 00 00 00 00 00 00 00 00 | ........
00007ffffffe008  | 00 00 00 00 00 00 00 00 | ........
00007ffffffe010  | 00 00 00 00 00 00 00 00 | ........
...              | ...
...              | ...
...              | ...
ffff800000000000 | 00 00 00 00 00 00 00 00 | ........
...              | ...
fffffffffffffff8 | 00 00 00 00 00 00 00 00 | ........
```

PROCESS

PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1

```
555555554000-555555555000 r--p  /bin/program
555555555000-555555556000 r-xp  /bin/program
...
7ffff7da6000-7ffff7dc8000 r--p  /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp  /lib/.../libc.so.6
...
7ffffffde000-7ffffffff000 rw-p  [stack]
```

# open

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The open() system call opens the file specified by pathname. If the specified file does not exist, it may optionally (if O_CREAT is specified in flags) be created by open().

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX    0x0000000000000000
RBX    0x0000000000000000
RCX    0x0000000000000000
RDX    0x0000000000000000
RDI    0x0000000000000000
RSI    0x0000000000000000
RSP    0x00007fffffffe010
RBP    0x0000000000000000
RIP    0x0000555555555000
```

MEMORY

```
555555554000    00 00 00 00 00 00 00 00 | ........
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

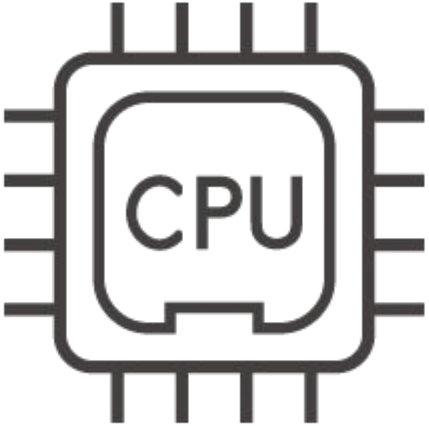
```
RAX   0x0000000000000000
RBX   0x0000000000000000
RCX   0x0000000000000000
RDX   0x0000000000000000
RDI   0x0000000000000000
RSI   0x0000000000000000
RSP   0x00007fffffffe010
RBP   0x0000000000000000
RIP   0x0000555555555000
```

MEMORY

```
555555554000   00 00 00 00 00 00 00 00 | ........
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



REGISTERS

RAX	0x0000000000000000
RBX	0x0000000000000000
RCX	0x0000000000000000
RDX	0x0000000000000000
RDI	**0x0000555555554000**
RSI	0x0000000000000000
RSP	0x00007fffffffe010
RBP	0x0000000000000000
RIP	**0x000055555555500a**

MEMORY

```
555555554000    00 00 00 00 00 00 00 00 | ........
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS	
RAX	0x0000000000000000
RBX	0x0000000000000000
RCX	0x0000000000000000
RDX	0x0000000000000000
RDI	0x0000555555554000
RSI	0x0000000000000000
RSP	0x00007fffffffe010
RBP	0x0000000000000000
RIP	0x000055555555500a

MEMORY

```
555555554000    00 00 00 00 00 00 00 00 | ........
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

RAX	0x00000067616c662f
RBX	0x0000000000000000
RCX	0x0000000000000000
RDX	0x0000000000000000
RDI	0x0000555555554000
RSI	0x0000000000000000
RSP	0x00007fffffffe010
RBP	0x0000000000000000
RIP	0x0000555555555014

MEMORY

```
555555554000    00 00 00 00 00 00 00 00 | ........
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX    0x00000067616c662f
RBX    0x0000000000000000
RCX    0x0000000000000000
RDX    0x0000000000000000
RDI    0x0000555555554000
RSI    0x0000000000000000
RSP    0x00007fffffffe010
RBP    0x0000000000000000
RIP    0x0000555555555014
```

MEMORY

```
555555554000    00 00 00 00 00 00 00 00 | ........
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX   0x00000067616c662f
RBX   0x0000000000000000
RCX   0x0000000000000000
RDX   0x0000000000000000
RDI   0x0000555555554000
RSI   0x0000000000000000
RSP   0x00007ffffffe010
RBP   0x0000000000000000
RIP   0x0000555555555017
```

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7ffffffe000    00 00 00 00 00 00 00 00 | ........
7ffffffe008    00 00 00 00 00 00 00 00 | ........
7ffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX    0x00000067616c662f
RBX    0x0000000000000000
RCX    0x0000000000000000
RDX    0x0000000000000000
RDI    0x0000555555554000
RSI    0x0000000000000000
RSP    0x00007fffffffe010
RBP    0x0000000000000000
RIP    0x0000555555555017
```

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX   0x00000067616c662f
RBX   0x0000000000000000
RCX   0x0000000000000000
RDX   0x0000000000000000
RDI   0x0000555555554000
RSI   0x0000000000000000
RSP   0x00007fffffffe010
RBP   0x0000000000000000
RIP   0x000055555555501e
```

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX    0x00000067616c662f
RBX    0x0000000000000000
RCX    0x0000000000000000
RDX    0x0000000000000000
RDI    0x0000555555554000
RSI    0x0000000000000000
RSP    0x00007ffffffe010
RBP    0x0000000000000000
RIP    0x000055555555501e
```

MEMORY

```
555555554000    2f 66 6c 61 67 00 00 00 | /flag...
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7ffffffe000     00 00 00 00 00 00 00 00 | ........
7ffffffe008     00 00 00 00 00 00 00 00 | ........
7ffffffe010     00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

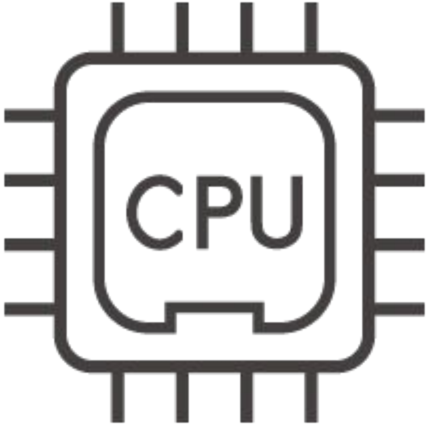
RAX	0x00000067616c662f
RBX	0x0000000000000000
RCX	0x0000000000000000
RDX	0x0000000000000000
RDI	0x0000555555554000
RSI	0x0000000000000000
RSP	0x00007fffffffe010
RBP	0x0000000000000000
RIP	0x0000555555555025

MEMORY

```
555555554000    2f 66 6c 61 67 00 00 00 | /flag...
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



REGISTERS

```
RAX   0x00000067616c662f
RBX   0x0000000000000000
RCX   0x0000000000000000
RDX   0x0000000000000000
RDI   0x0000555555554000
RSI   0x0000000000000000
RSP   0x00007fffffffe010
RBP   0x0000000000000000
RIP   0x0000555555555025
```

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

RAX	0x0000000000000002
RBX	0x0000000000000000
RCX	0x0000000000000000
RDX	0x0000000000000000
RDI	0x0000555555554000
RSI	0x0000000000000000
RSP	0x00007fffffffe010
RBP	0x0000000000000000
RIP	0x000055555555502c

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX    0x0000000000000002
RBX    0x0000000000000000
RCX    0x0000000000000000
RDX    0x0000000000000000
RDI    0x0000555555554000
RSI    0x0000000000000000
RSP    0x00007fffffffe010
RBP    0x0000000000000000
RIP    0x000055555555502c
```

MEMORY

```
555555554000    2f 66 6c 61 67 00 00 00 | /flag...
555555554008    00 00 00 00 00 00 00 00 | ........
555555554010    00 00 00 00 00 00 00 00 | ........
...             ...
555555555000    48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008    00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010    67 00 00 00 48 89 07 48 | g...H..H
555555555018    c7 c6 00 00 00 00 48 c7 | ......H.
555555555020    c2 00 00 00 00 48 c7 c0 | .....H..
555555555028    02 00 00 00 0f 05 00 00 | ........
...             ...
7fffffffe000    00 00 00 00 00 00 00 00 | ........
7fffffffe008    00 00 00 00 00 00 00 00 | ........
7fffffffe010    00 00 00 00 00 00 00 00 | ........
```

open("/flag", O_RDONLY, 0)

MEMORY

```
0000555555554000   2f 66 6c 61 67 00 00 00 | /flag...
0000555555554008   00 00 00 00 00 00 00 00 | ........
0000555555554010   00 00 00 00 00 00 00 00 | ........
...                ...
0000555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
0000555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
0000555555555010   67 00 00 00 48 89 07 48 | g...H..H
0000555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
0000555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
0000555555555028   02 00 00 00 0f 05 00 00 | ........
...                ...
00007fffffffe000   00 00 00 00 00 00 00 00 | ........
00007fffffffe008   00 00 00 00 00 00 00 00 | ........
00007fffffffe010   00 00 00 00 00 00 00 00 | ........
...                ...
...                ...
...                ...
ffff800000000000   00 00 00 00 00 00 00 00 | ........
...                ...
ffff????????????   ?? ?? ?? ?? ?? ?? ?? ?? | ........
...                ...
fffffffffffffff8   00 00 00 00 00 00 00 00 | ........
```

PROCESS	
PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1

```
555555554000-555555555000 r--p  /bin/program
555555555000-555555556000 r-xp  /bin/program
...
7ffff7da6000-7ffff7dc8000 r--p  /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp  /lib/.../libc.so.6
...
7ffffffde000-7ffffffff000 rw-p  [stack]
```

open("/flag", O_RDONLY, 0)

MEMORY

```
0000555555554000   2f 66 6c 61 67 00 00 00 | /flag...
0000555555554008   00 00 00 00 00 00 00 00 | ........
0000555555554010   00 00 00 00 00 00 00 00 | ........
...                ...
0000555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
0000555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
0000555555555010   67 00 00 00 48 89 07 48 | g...H..H
0000555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
0000555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
0000555555555028   02 00 00 00 0f 05 00 00 | ........
...                ...
00007ffffffde000   00 00 00 00 00 00 00 00 | ........
00007ffffffde008   00 00 00 00 00 00 00 00 | ........
00007ffffffde010   00 00 00 00 00 00 00 00 | ........
...                ...
...                ...
...                ...
ffff800000000000   00 00 00 00 00 00 00 00 | ........
...                ...
ffff????????????   ?? ?? ?? ?? ?? ?? ?? ?? | ........
...                ...
fffffffffffffff8   00 00 00 00 00 00 00 00 | ........
```

PROCESS

PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 ... FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1 **/flag**

```
555555554000-555555555000 r--p  /bin/program
555555555000-555555556000 r-xp  /bin/program
...
7ffff7da6000-7ffff7dc8000 r--p  /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp  /lib/.../libc.so.6
...
7ffffffde000-7ffffffff000 rw-p  [stack]
```

open("/flag", O_RDONLY, 0)

```
mov rdi, 0x555555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

REGISTERS

```
RAX   0x0000000000000003
RBX   0x0000000000000000
RCX   0x0000000000000000
RDX   0x0000000000000000
RDI   0x0000555555554000
RSI   0x0000000000000000
RSP   0x00007fffffffe010
RBP   0x0000000000000000
RIP   0x000055555555502e
```

MEMORY

```
555555554000   2f 66 6c 61 67 00 00 00 | /flag...
555555554008   00 00 00 00 00 00 00 00 | ........
555555554010   00 00 00 00 00 00 00 00 | ........
...            ...
555555555000   48 bf 00 40 55 55 55 55 | H..@UUUU
555555555008   00 00 48 b8 2f 66 6c 61 | ..H./fla
555555555010   67 00 00 00 48 89 07 48 | g...H..H
555555555018   c7 c6 00 00 00 00 48 c7 | ......H.
555555555020   c2 00 00 00 00 48 c7 c0 | .....H..
555555555028   02 00 00 00 0f 05 00 00 | ........
...            ...
7fffffffe000   00 00 00 00 00 00 00 00 | ........
7fffffffe008   00 00 00 00 00 00 00 00 | ........
7fffffffe010   00 00 00 00 00 00 00 00 | ........
```

# System Calls

SYSCALL NAME	RAX	ARG0 (rdi)	ARG1 (rsi)	ARG2 (rdx)	ARG3 (r10)	ARG4 (r8)	ARG5 (r9)
read	0	int fd	char *buf	size_t count	-	-	-
write	1	int fd	char *buf	size_t count	-	-	-
open	2	char *filename	int flags	umode_t mode	-	-	-
close	3	int fd	-	-	-	-	-
mmap	9	long addr	size_t len	long prot	int flags	int fd	off_t offset
mprotect	A	long addr	size_t len	long prot	-	-	-
munmap	B	long addr	size_t len	-	-	-	-
getpid	27	-	-	-	-	-	-
fork	39	-	-	-	-	-	-
execve	3B	char *filename	char **argv	char **envp	-	-	-
exit	3C	int error_code	-	-	-	-	-
getcwd	4F	char *buf	size_t size	-	-	-	-
chdir	50	char *filename	-	-	-	-	-
chmod	5A	char *filename	umode_t mode	-	-	-	-
gettimeofday	60	struct timeval *tv	struct timezone *tz	-	-	-	-
getuid	66	-	-	-	-	-	-
geteuid	6B	-	-	-	-	-	-
getppid	6E	-	-	-	-	-	-

For more system calls, see https://x64.syscall.sh/