

神奇的strace

CIH<Software Magician>

IamCIH@gmail.com

2008/12/13

工作目錄API

```
# pwd
```

```
/tmp/cih
```

```
# strace -o xxx    pwd
```

```
# grep cih xxx
```

```
getcwd("/tmp/cih", 4096)           = 9
```

```
write(1, "/tmp/cih\n", 9)         = 9
```

```
# man getcwd
```

SYNOPSIS

```
#include <unistd.h>
```

```
char *getcwd(char *buf, size_t size);
```

設定最多可同時開啟檔案個數API

```
# strace -o xxx sh
# ulimit -n 5566
# exit
# grep 5566 xxx
write(2, "\10\10\10\10ulimit -n 5566", 18) = 18
setrlimit(RLIMIT_NOFILE, {rlim_cur=5566, rlim_max=5566}) = 0
write(4, "ulimit -n 5566\nexit\n", 20) = 20
```

改成C的版本如下：

```
struct rlimit rlim = {.rlim_cur=5566, .rlim_max=5566};
setrlimit(RLIMIT_NOFILE, &rlim);
```

讀取系統時間日期API

```
# strace -o xxx    date
```

```
# strace -o yyy    date
```

```
# diff -ruN xxx yyy
```

```
-clock_gettime(CLOCK_REALTIME, {1228950290,  
    953102720}) = 0
```

```
+clock_gettime(CLOCK_REALTIME, {1228950294,  
    261772376}) = 0
```

改成C的版本如下：

```
struct timespec tp;
```

```
clock_gettime(CLOCK_REALTIME, &tp);
```

找到clock_gettime這個System Call在Linux kernel source裡面

```
# grep -rw sys_clock_gettime /usr/src/linux  
/usr/src/linux/kernel/posix-timers.c:
```

```
sys_clock_gettime(const clockid_t which_clock,  
                  struct timespec __user *tp)
```

改成Linux kernel的版本如下：

```
struct timespec tp;  
old_fs=get_fs();  
set_fs(KERNEL_DS);  
sys_clock_gettime(CLOCK_REALTIME, &tp);  
set_fs(old_fs);
```



Thank you !

Kat Digital Corp.

3F-5, No.66, SanChong Rd. NanGang Taipei 115, Taiwan

Phone: 886 2 6617 3168

Website: www.katdc.com