Checking the information of OS

```
lap@lap-vm:~$ uname -a
Linux lap-vm 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00
:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
lap@lap-vm:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.1 LTS"
lap@lap-vm:~$
```

Compile the kernel

Before starting to compile you need to install a few packages. Type the following commands in your terminal:

```
sudo apt-get install gcc
sudo apt-get install libncurses5-dev
sudo apt-get install bison
sudo apt-get install flex
sudo apt-get install libssl-dev
sudo apt-get install libelf-dev
sudo apt-get update


or
```

```
apt-get install gcc libncurses5-dev bison flex libssl-dev
libelf-dev update -y
```

Get kernel

```
lap@lap-vm:~$ pwd
/home/lap
lap@lap-vm:~$ wget http://cdn.kernel.org/pub/linux/kernel/
v4.x/linux-4.4.2.tar.gz
```

Extract the kernel source code

```
root@lap-vm:~# tar -xzvf linux-4.4.2.tar.gz
```

Define a new system call pidtoname

```
root@lap-vm:~# cd linux-4.4.2/
root@lap-vm:~/linux-4.4.2# mkdir pnameid
root@lap-vm:~/linux-4.4.2# cd pnameid/
root@lap-vm:~/linux-4.4.2/pnameid# touch pnameid.c pnameid
.h Makefile
```

Content pnameid.h file

```
root@lap-vm:~/linux-4.4.2/pnameid# cat pnameid.h

asmlinkage long sys_pnametoid(char* name);
```

Content pnameid.c file

```
root@lap-vm:~/linux-4.4.2/pnameid# cat pnameid.c

#include <linux/syscalls.h>

#include <linux/kernel.h>

#include <linux/sched.h>

#include <linux/init.h>

#include <linux/string.h>

#include "pnameid.h"

asmlinkage long sys_pnametoid(char* name){

    char buf[32];

    strncpy_from_user(buf, name, sizeof(buf));

    printk("DEBUG: %s", buf);

    struct task_struct *task;

    int pid = -1;

    for_each_process(task){

        if(strcmp(task->comm,buf) == 0){

            pid = task->pid;

        }

    }

    return (long)pid;

}
```

Content Makefile file

```
root@lap-vm:~/linux-4.4.2/pnameid# cat Makefile
obj-y := pnameid.o
```

Update Makefile to build Kernel

```
root@lap-vm:~/linux-4.4.2/pnameid# cd ..
root@lap-vm:~/linux-4.4.2# vim Makefile
root@lap-vm:~/linux-4.4.2# cat Makefile | grep "core-y"
core-y          := usr/
core-y          += kernel/ certs/ mm/ fs/ ipc/ security/ crypto/ block/ pnameid/
                $(core-y) $(core-m) $(drivers-y) $(drivers-m) \
root@lap-vm:~/linux-4.4.2# vim arch/x86/entry/syscalls/syscall_64.tbl
root@lap-vm:~/linux-4.4.2#
root@lap-vm:~/linux-4.4.2# cat arch/x86/entry/syscalls/syscall_64.tbl | grep pnametoid -C 3
323 common  userfaultfd     sys_userfaultfd
324 common  membarrier      sys_membarrier
325 common  mlock2          sys_mlock2
326 64  pnametoid        sys_pnametoid
#
# x32-specific system call numbers start at 512 to avoid cache impact
```

```
# for native 64-bit operation.

root@lap-vm:~/linux-4.4.2# cat include/linux/syscalls.h |
grep pnametoid -C 3
asmlinkage long sys_membarrier(int cmd, int flags);


asmlinkage long sys_mlock2(unsigned long start, size_t len
, int flags);
asmlinkage long sys_pnametoid(char* name);
#endif
root@lap-vm:~/linux-4.4.2#
```

Compile and install the kernel:

```
root@lap-vm:~/linux-4.4.2# make menuconfig
root@lap-vm:~/linux-4.4.2# make -j4
root@lap-vm:~/linux-4.4.2# make modules_install install
```

Checking new kernel

```
lap@lap-vm:~$ uname -a
Linux lap-vm 4.4.2 #1 SMP Tue Apr 30 07:32:43 ICT 2019 x86
_64 x86_64 x86_64 GNU/Linux
```

Test the pnameid system call

```
lap@lap-vm:~$ pwd
/home/lap
lap@lap-vm:~$ cat test.c
#include<stdio.h>
#include<linux/kernel.h>
#include<sys/syscall.h>
#include<unistd.h>
#include<string.h>
#define MAX_SIZE 32
int main()
{
    // Test syscall pnametoid
    char name[32];
    puts("Enter process to find");
    scanf("%s",name);
    long int status = syscall(326, name);
    printf("sys_pnametoid returned %ld\n", status);
    return 0;
}
lap@lap-vm:~$ gcc test.c

lap@lap-vm:~$ ps -ef | grep compiz
lap         6138    5700  6 08:03 ?        00:00:26 compiz
lap         6964    6814  0 08:10 pts/3    00:00:00 grep --c
olor=auto compiz
lap@lap-vm:~$
lap@lap-vm:~$ ./a.out
```

```
Enter process to find

compiz

sys_pnametoid returned 6138


lap@lap-vm:~$ ps -ef | grep perf

root            28        2  0 08:02 ?        00:00:00 [perf]

lap           6974    6814  0 08:12 pts/3    00:00:00 grep --c

olor=auto perf

lap@lap-vm:~$

lap@lap-vm:~$ ./a.out

Enter process to find

perf

sys_pnametoid returned 28

lap@lap-vm:~$

lap@lap-vm:~$ dmesg | grep "DEBUG"

[  285.082165] DEBUG: ssh

[  293.566342] DEBUG: bash

[  437.508873] DEBUG: sshDEBUG: compiz

[  609.100889] DEBUG: perf
```