

# [TOOL] Anti-Ptrace Linux LKM

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0090.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/30/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 30 Mar 2003 15:57:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office  
housewarming rates on automated network vulnerability  
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Anti-Ptrace Linux LKM

---

## DETAILS

The following Linux LKM allows an administrator to disable the ptrace abilities under the 2.4.x kernels.

Tool source:

```
#!/bin/sh
```

```
# MAKE ME EXECUTABLE !!!
```

```
#
```

```
# root@Hogwarts:/home/sacrine/TEST# chmod +x anti-ptrace
```

```
# root@Hogwarts:/home/sacrine/TEST# ./anti-ptrace
```

```
# [+] making anti-ptrace.c: OK
```

```
# [+] compiling the script: OK
```

```
# [+] loading the module : OK
```

```
#
```

```
echo -n " [+] making anti-ptrace.c: "
```

```
cat > anti-ptrace.c <<NETRIC
```

```
/*
```

## Securiteam: [TOOL] Anti-Ptrace Linux LKM

```
* Noodoplossing voor de ptrace race vuln
* anti_ptrace.c by sacrine
* netric.org
*/
```

```
#define __KERNEL__
#define MODULE
#define LINUX

#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/types.h>
#include <linux/version.h>
#include <linux/slab.h>
#include <linux/sched.h>
#include <linux/fs.h>
#include <linux/ctype.h>
#include <linux/tty.h>
#include <sys/syscall.h>

#include <linux/ptrace.h>

long (*o_ptrace) ( pid_t pid,
    void *addr,
    void *data );

extern void* sys_call_table[];

int anti_ptrace( pid_t pid,
    uid_t uid,
    void *addr,
    void *data )
{
    uid_t o_uid;

    if(current->uid == 0)
    {
        return(o_ptrace(pid,addr,data));
    }

    printk("warning: ptrace(); violation\n"
        "pid=[%i] uid=[%i]\n"
        ,current->pid
        ,current->uid);

    console_print("warning: non-root users are not allowed to use
ptrace();\n");
    return EPERM;
}
```

## Securiteam: [TOOL] Anti-Ptrace Linux LKM

```
int init_module(void)
{
    o_ptrace=sys_call_table[SYS_ptrace];
    sys_call_table[SYS_ptrace]=anti_ptrace;

    printk("anti-ptrace kernel module loaded with pid=[%i]\n",
    current->pid);

    return(0);
}

void cleanup_module(void)
{
    sys_call_table[SYS_ptrace]=o_ptrace;
    printk("anti-ptrace kernel module ended with pid=[%i]\n",
    current->pid);
}
```

```
NETRIC
echo "OK";
echo -n " [+] compiling the script: ";
gcc -c anti_ptrace.c -I/lib/modules/$(uname -r)/build/include
echo "OK";
echo -n " [+] loading the module : ";
/sbin/insmod anti_ptrace.o >/dev/null
echo "OK";
```

# sacrine [Netric Security]

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[sacrine@netric.org](mailto:sacrine@netric.org)> sacrine.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.