Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Nuevo modulo para el kernel: asterix.o (6500 lectures)

Per **Guillem Cantallops Ramis**, ***Beowulf*** (http://bulma.net/beowulf/)

Creado el 04/02/2001 00:00 modificado el 04/02/2001 00:00

Guardadlo para el 28 de diciembre proximo, solo sirve para gastar bromas ;-)

Bueno, leyendo un articulo de Nitesh Dhanjani y Gustavo Rodriguez-Rivera en la LinuxJournal[1] de febrero de 2001, se me ocurrió hacerle algunas modificaciones a uno de sus ejemplos y salió esto...

```
/* gcc -Wall -DMODULE -D__KERNEL__ -DLINUX -c asterix.c */

#include <linux/kernel.h>
#include <linux/module.h>
#include <sys/syscall.h>

extern void *sys_call_table[];

asmlinkage int (*original_sys_delete_module)(const char *);

asmlinkage int fake_sys_delete_module(const char *s)
{
  static int conya=0;

  if (
    (s[0]=='a')&&
    (s[1]=='s')&&
    (s[2]=='t')&&
    (s[3]=='e')&&
    (s[4]=='r')&&
    (s[5]=='i')&&
    (s[6]=='x')&&
    (s[7]=='\0')
  ) {
    printk("Asterix el Galo jamás se rinde, romanos ]:-)\n");
    conya=conya%128+1;
    return -conya;
  }
  else {
    return original_sys_delete_module(s);
  }
}

int init_module()
{
  printk("Asterix el Galo tomando el control de su destino... ");
  original_sys_delete_module=sys_call_table[__NR_delete_module];
  sys_call_table[__NR_delete_module]=fake_sys_delete_module;
  printk("OK!\n");
  return 0;
}

void cleanup_module()
{
  sys_call_table[__NR_delete_module]=original_sys_delete_module;
  printk("IMPOSIBLE! Asterix el Galo ha sido vencido!!!\n");
}
```

Después de compilarlo basta ejecutar `insmod asterix.o` para cargarlo.

Se trata del código para un módulo del kernel (llamado Asterix, el irreductible Galo :-) que intercepta la system call delete_module(). Si el módulo que se quiere borrar tiene un nombre distinto del suyo, todo va como siempre. Pero si intentan borrarlo a el, muestra un error cualquiera y evita la ejecución de dicha system call.

La verdad es que si sois varios administrando una máquina es genial para gastar bromas, y además es completamente inofensivo (aunque yo no me hago responsable de nada) y ocupa menos de 1KB. Imaginaos la cara que se le pone al administrador de turno cuando ve que no hay perra forma de descargar el módulo 'asterix', que además le da cada vez un error diferente y sin ningúna relación... Seguro que es para hacerle una foto X'-DDD

Lista de enlaces de este artículo:

1. http://linuxjournal.com

E-mail del autor: beowulf _ARROBA_ bulma.net