PB167 /PB167/ Cvicenie #3 Linux Kernel modules

1. uistit sa o pritomnosti suboru C:\PB167\Fedora12proPB167.vdi
Ak neexistuje, stiahnut z ISu:
https://is.muni.cz/auth/el/1433/jaro2013/PB167/um/cv2/Fedora12proPB167.vdi

2. Image skopirujeme do svojho sukromneho adresara (v ziadnom pripade nepouzivame tento original, ale svoju kopiu)

3. Vytvorime virtualny stroj s existujucim diskom (Fedora12proPB167.vdi) a zapnutou podporou PAE (Settings -> System -> Processor)

4. Stiahneme subor z ISu:
https://is.muni.cz/auth/el/1433/jaro2013/PB167/um/cv3/km.iso

Obsahuje CD image so subormi, ktore budeme vo VM potrebovat. Toto ISO pripojime ako CDROM vo VirtualBox-e k nasemu VM.
(Settings -> Storage -> Controller: IDE -> CD icon right click -> Choose a virtual CD/DVD drive

5. Nabootujeme VM. root:OperacniSystemy

6. Pripojenie CD
mount /dev/sr0 /mnt/cdrom

7. sprovoznenie siete
ifconfig -a

dhclient eth2
ping muni.cz

8. dodatocna instalacia balikov
yum install -y openssh-clients strace ltrace rsync vim

9. CD je read only, kopirovanie do svojho adresara
rsync -a /mnt/cdrom /root

10. instalace zdrojovych suborov jadra pre kompilaciu modulov
yum install --disablerepo=updates kernel-PAE-devel

11. zavedenie modulu do jadra
insmod emptymodul.ko

12. informacie o module
modinfo emptymodul.ko

13. odstranenie modulu z jadra
rmmod emptymodul.ko

14. Vypis dissasemlovania objektoveho suboru:
objdump -Dslx emptymodul.o > emptymodul.diss
vim emptymodul.diss

cat /dev/chardev
echo ‘hi’ > /dev/chardev

Nahranie na aisu:

man scp
scp ZDROJ xlogin@aisa.fi.muni.cz:/home/xlogin/CIEL

==========

* Sledovanie systemovych volani, ktore vykonava program (syscall())
strace df

* Sledovanie volani funkcii glibc (printf...)
ltrace df

Skuste si strace/ltrace na nasledovny program (mali sme na 2. cviceni):

```
#include <stdio.h>
#include <unistd.h>
#include <sys/syscall.h>

int main(void)
{
  int uid;
  uid = syscall(20);
  printf("UID = %d\n", uid);
  return 0;
}
```

==========

Literatura:

http://dl.packetstormsecurity.net/docs/hack/LKM_HACKING.html
http://www.ibm.com/developerworks/linux/library/l-kernel-memory-access/index.html
http://www.ibm.com/developerworks/library/l-system-calls/
http://tldp.org/LDP/lkmpg/2.6/html/index.html