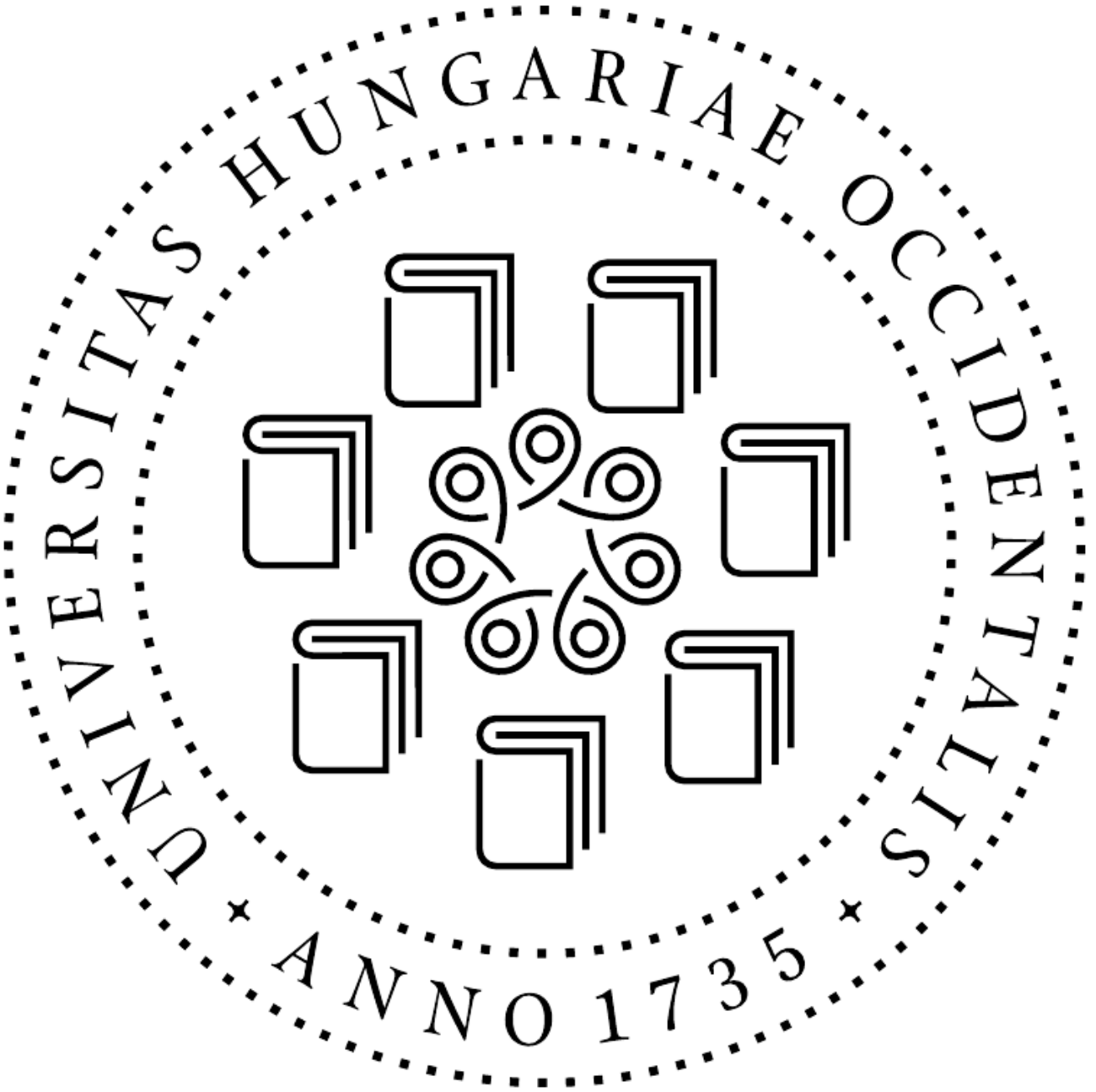

UNIVERSITAS HUNGARIAE OCCIDENTALIS
ANNO 1735

A UNIX rendszerek biztonsági modellje kezdetben

- A root (0-ás UID-ű) processzek korlátozás nélkül dolgozhatnak a kernel rendszerhívásaival

- Minden más processz korlátozott jogokkal rendelkezik.

- A processzek már kezdetben is rendelkeznek személyiséggel/szerepkörrel, ezek az UID/GID azonosítók.

- rxwrwxrwx formátumú DAC fájlrendszerjogosultságok

A DAC biztonsági modell kibővülése

- Setuid, setgid, sticky bitek
- Kiegészítő csoporttagság
- RUID/EUID/SUID(/FSUID) – RGID/EGID/SGID(/FSGID)
- POSIX ACL-ek (vagy NFSv4 ACL-ek)
- A mindenható root jog feldarabolása (Linux Capabilities)
- Filesystem capabilities

```
P'(permitted) = (P(inheritable) & F(inheritable)) |
                (F(permitted) & cap_bset)
P'(effective) = F(effective) ? P'(permitted) : 0
P'(inheritable) = P(inheritable)
```

/home/tamas : bash

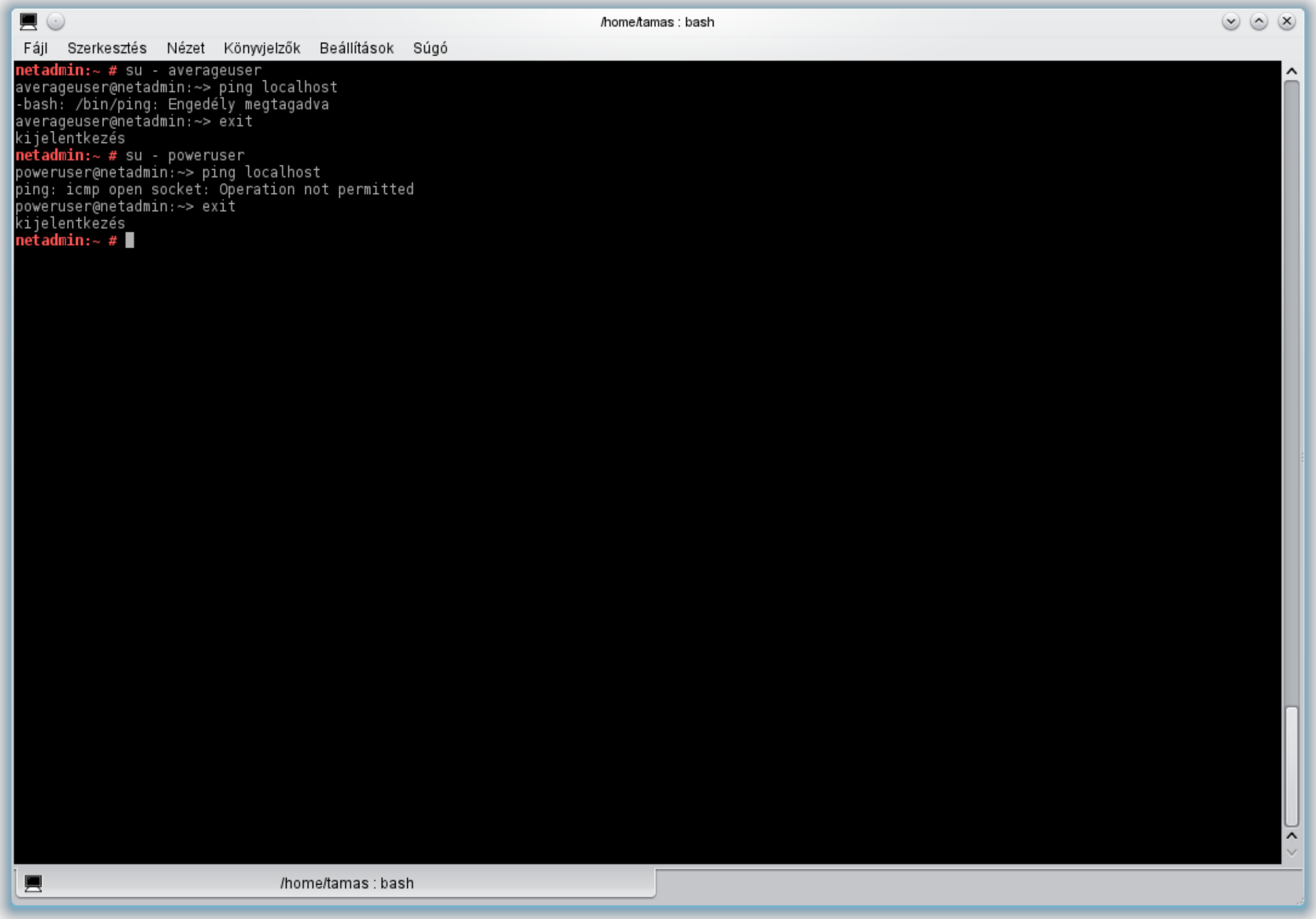
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó

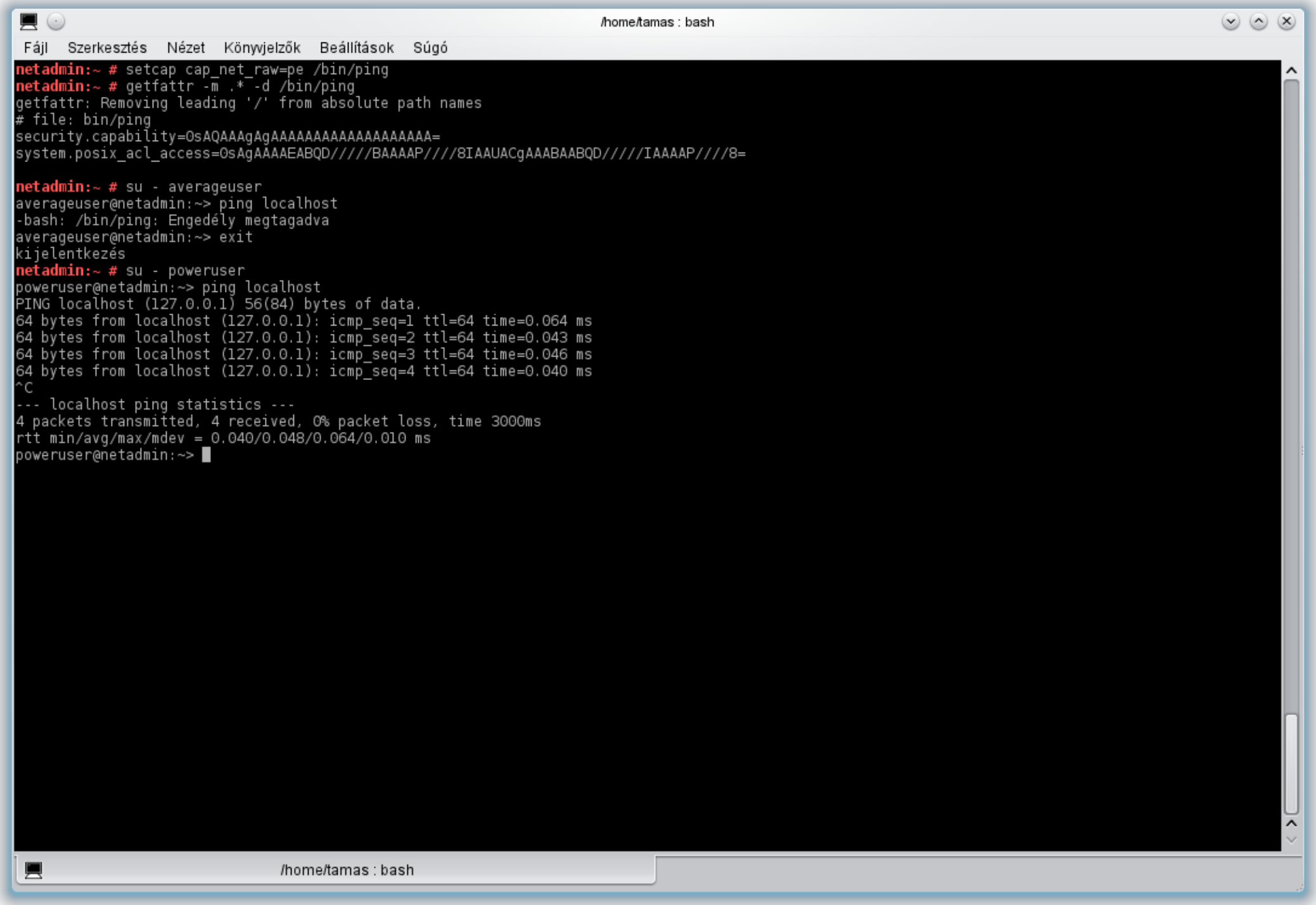
```
netadmin:~ # useradd -m -g users averageuser
netadmin:~ # useradd -m -g wheel poweruser
netadmin:~ # ls -l /bin/ping
-rwsr-xr-x 1 root root 39992 Oct 29  2011 /bin/ping
netadmin:~ # chmod 500 /bin/ping
netadmin:~ # ls -l /bin/ping
-r-x------ 1 root root 39992 Oct 29  2011 /bin/ping
netadmin:~ # su - averageuser
averageuser@netadmin:~> ping localhost
-bash: /bin/ping: Engedély megtagadva
averageuser@netadmin:~> exit
kijelentkezés
netadmin:~ # su - poweruser
poweruser@netadmin:~> ping localhost
-bash: /bin/ping: Engedély megtagadva
poweruser@netadmin:~> exit
kijelentkezés
netadmin:~ # setfacl -m g:wheel:rx /bin/ping
netadmin:~ # getfacl /bin/ping
getfacl: Removing leading '/' from absolute path names
# file: bin/ping
# owner: root
# group: root
user::r-x
group::---
group:wheel:r-x
mask::r-x
other::---

netadmin:~ # getfattr -m .* -d /bin/ping
getfattr: Removing leading '/' from absolute path names
# file: bin/ping
system.posix_acl_access=0sAgAAAAEABQD/////BAAAAP////8IAAUACgAAABAABQD/////IAAAAP////8=

netadmin:~ # stat /bin/ping
  File: `/bin/ping'
  Size: 39992           Blocks: 80         IO Block: 4096   regular file
Device: 802h/2050d      Inode: 2097261     Links: 1
Access: (0550/-r-xr-x---)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2013-03-11 19:05:33.030454798 +0100
Modify: 2011-10-29 19:04:20.000000000 +0200
Change: 2013-03-12 09:35:03.754210650 +0100
 Birth: -
netadmin:~ #
```

/home/tamas : bash


/home/tamas : bash
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
netadmin:~ # su - averageuser
averageuser@netadmin:~> ping localhost
-bash: /bin/ping: Engedély megtagadva
averageuser@netadmin:~> exit
kijelentkezés
netadmin:~ # su - poweruser
poweruser@netadmin:~> ping localhost
ping: icmp open socket: Operation not permitted
poweruser@netadmin:~> exit
kijelentkezés
netadmin:~ #
/home/tamas : bash


/home/tamas : bash
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
netadmin:~ # setcap cap_net_raw=pe /bin/ping
netadmin:~ # getfattr -m .* -d /bin/ping
getfattr: Removing leading '/' from absolute path names
# file: bin/ping
security.capability=0sAQAAAgAgAAAAAAAAAAAAAAAAAAA=
system.posix_acl_access=0sAgAAAAEABQD/////BAAAAP////8IAAUACgAAABAABQD/////IAAAAP////8=
netadmin:~ # su - averageuser
averageuser@netadmin:~> ping localhost
-bash: /bin/ping: Engedély megtagadva
averageuser@netadmin:~> exit
kijelentkezés
netadmin:~ # su - poweruser
poweruser@netadmin:~> ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.064 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.040 ms
^C
--- localhost ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.040/0.048/0.064/0.010 ms
poweruser@netadmin:~>
/home/tamas : bash

A cron démon számára olyan biztonsági megoldást kerestem, amelynél a közönséges felhasználók ütemezett feladatai szűkebb jogkörökkel futnak, mint a rendszer ütemezett feladatai, vagy ugyanazon felhasználók shell (vagy apache-itk, stb.) munkamenetei.

```
pid = fork();

if (pid == 0)
{
    // gyerekprocessz
    setuid (n);
    execve(argv[1], argv+1, envp);
}
else
{
    // szülőprocessz
    ...
}
```

Más szóval, ne csak a setuid (vagy SETUID/SETGID fájlok végrehajtása), hanem az execve hívások is hassanak a processzek jogosultságára.

Erre a célra olyan UNIX DAC rendszert tartanék ideálisnak, amelynél:

- Az UID és GID értékek közös névtérbe vannak, tehát csak egyféle identitás létezik: a szerep.

- A szerepek és a root jogot alkotó capabilityk is közös névtérben vannak.

- A execve hívásokkor történő szerep-hozzáadás és elvétel a meglevő filesystem capabilityknél finomabban szabályozható.

- A fájlok hozzáférés-vezérlését a jelenleginél kifinomultabb, átörökíthető ACL-ek szabályozzák.

- Az öröklés rendjének egyértelművé tétele érdekében a symlinkek megszűnnek.

Mivel ilyen nincs, és nem is lesz, MAC rendszert kell használnom:

Olyan MAC megoldást kerestem, ahol:

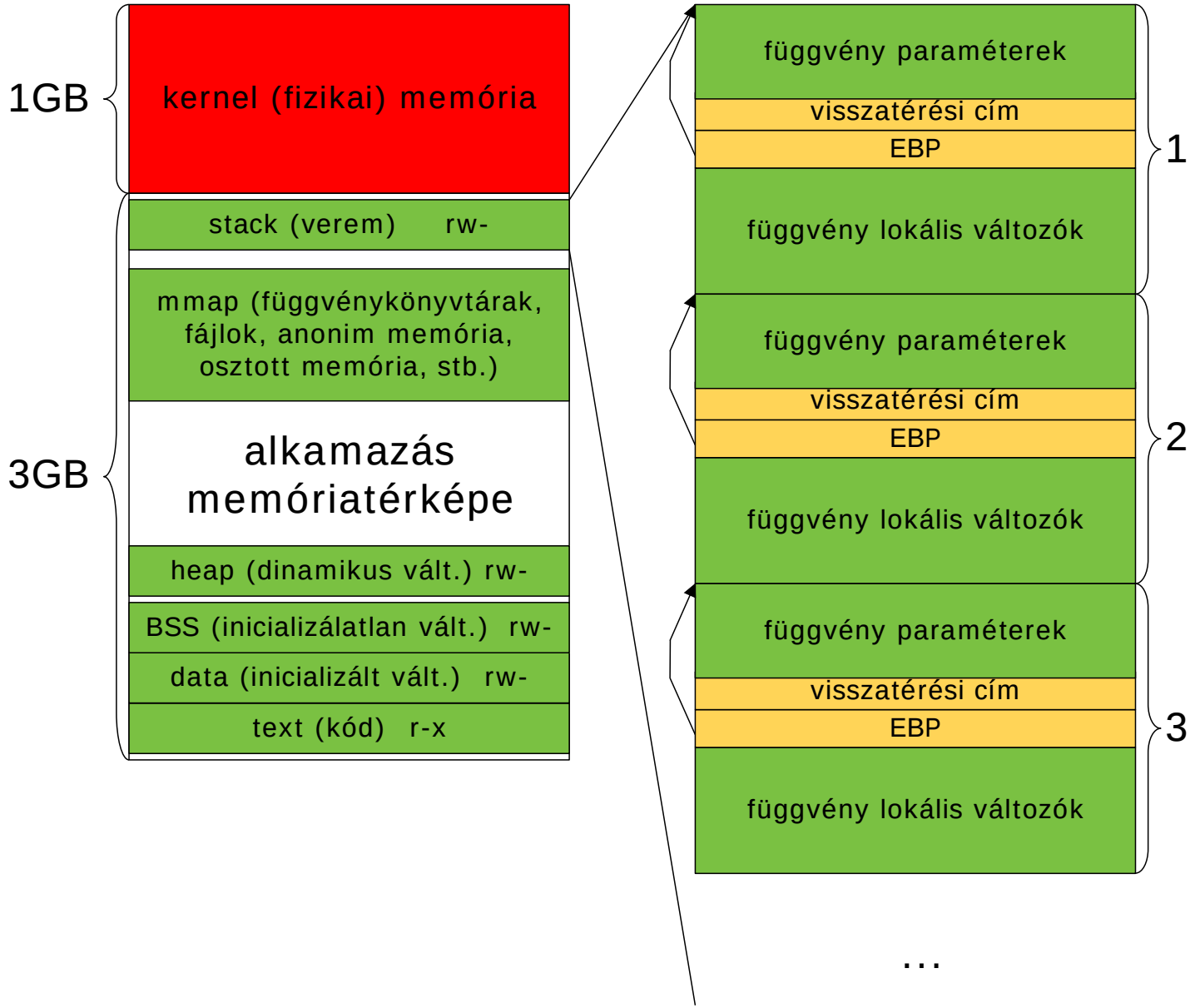
1. Az A user nevében futó x bináris más jogkörrel rendelkezhet, mint az A user nevében futó y bináris.

2. Az A user nevében futó x bináris más jogkörrel rendelkezhet, mint a B user nevében futó x bináris.

3. a processz jogköre ne csak vagy az UID/GID vagy a futó bináris fájl függvénye lehessen, hanem egy időben a kettő kombinációjáé.

Ha MAC, akkor:

PaX - védelem a processzek memóriatérképének korrupciója ellen



A PaX főbb funkciói

-NOEXEC : Az ExeShieldhez és az W^X-hez hasonlóan a processzek virtuális memóriatérképének nem végrehajthatóként megjelölt lapjairól valóban megtiltja utasításkódok beolvasását, még akkor is, ha a a processzor ezt hardveresen nem támogatja!

-SEGMEXEC : A CPU szegmentálási logikáján alapuló NX-bit emuláció

-PAGEEXEC : A CPU lapozási logikáján alapuló NX-bit emuláció vagy a hardveres NX-bit kihasználása.

-ASLR : Eredetileg a PaX team találmánya. 2001 óta alkalmazzák, máig a legátfogóbb, és legnagyobb véletlenszerűséget biztosító megoldás.

-MPROTECT: Kikényszeríti, hogy a processzeknek egyszerre írható és végrehajtható memórialapjai legyenek: lehetetlenné teszi, hogy a programok módosítsák vagy bővítsék magukat.

/home/tamas : bash

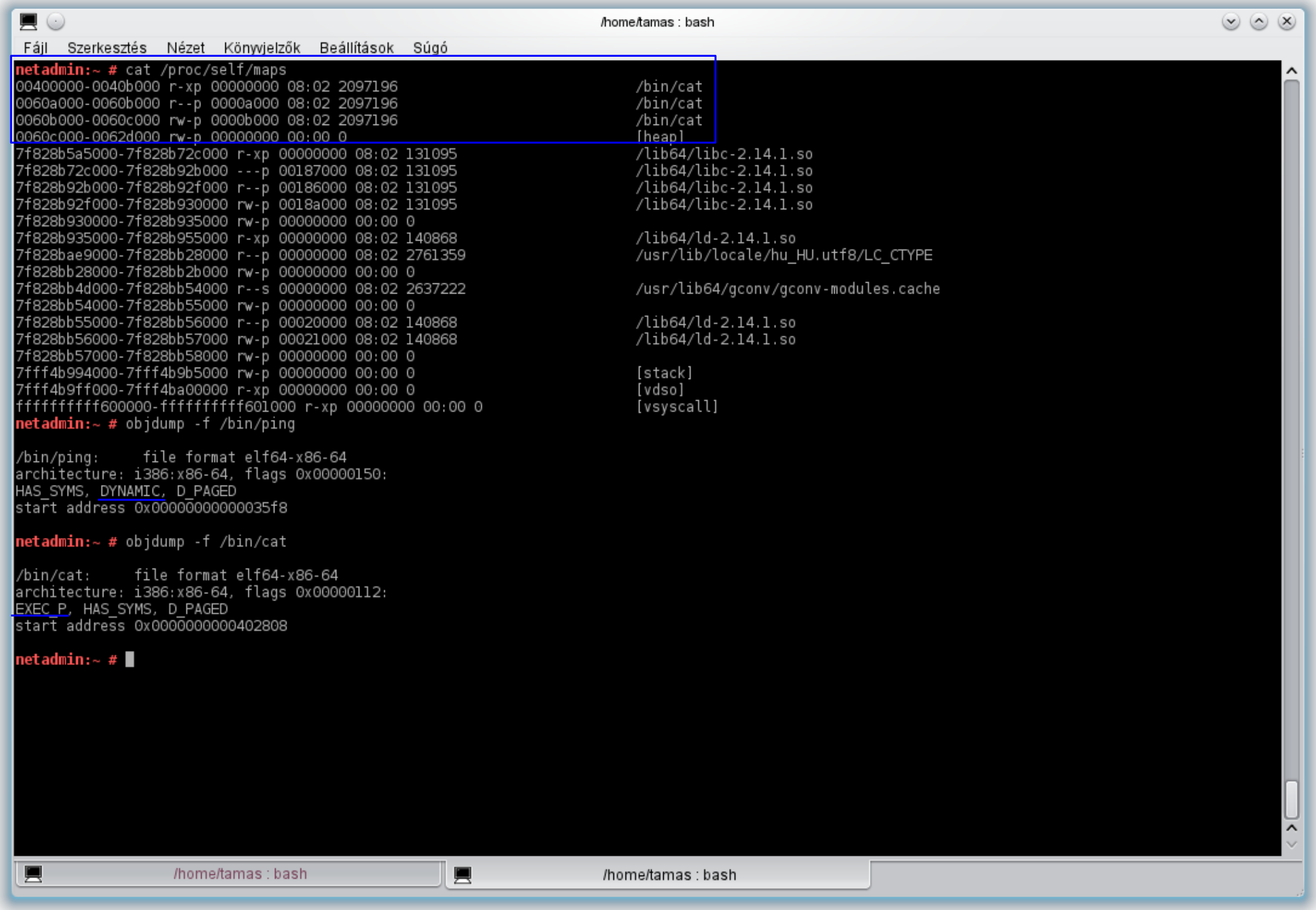
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó

```
poweruser@netadmin:~> ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.070 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.063 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.070 ms
^C
--- localhost ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.046/0.062/0.070/0.011 ms
poweruser@netadmin:~>
```

/home/tamas : bash /home/tamas : bash

```
netadmin:~ # ps -A | grep ping
 7892 pts/1    00:00:00 ping
netadmin:~ # cat /proc/7892/maps
7ff4e855e000-7ff4e856a000 r-xp 00000000 08:02 169134                     /lib64/libnss_files-2.14.1.so
7ff4e856a000-7ff4e8769000 ---p 0000c000 08:02 169134                     /lib64/libnss_files-2.14.1.so
7ff4e8769000-7ff4e876a000 r--p 0000b000 08:02 169134                     /lib64/libnss_files-2.14.1.so
7ff4e876a000-7ff4e876b000 rw-p 0000c000 08:02 169134                     /lib64/libnss_files-2.14.1.so
7ff4e876b000-7ff4e88f2000 r-xp 00000000 08:02 131095                     /lib64/libc-2.14.1.so
7ff4e88f2000-7ff4e8af1000 ---p 00187000 08:02 131095                     /lib64/libc-2.14.1.so
7ff4e8af1000-7ff4e8af5000 r--p 00186000 08:02 131095                     /lib64/libc-2.14.1.so
7ff4e8af5000-7ff4e8af6000 rw-p 0018a000 08:02 131095                     /lib64/libc-2.14.1.so
7ff4e8af6000-7ff4e8afb000 rw-p 00000000 00:00 0
7ff4e8afb000-7ff4e8aff000 r-xp 00000000 08:02 134788                     /lib64/libcap.so.2.22
7ff4e8aff000-7ff4e8cfe000 ---p 00004000 08:02 134788                     /lib64/libcap.so.2.22
7ff4e8cfe000-7ff4e8cff000 r--p 00003000 08:02 134788                     /lib64/libcap.so.2.22
7ff4e8cff000-7ff4e8d00000 rw-p 00004000 08:02 134788                     /lib64/libcap.so.2.22
7ff4e8d00000-7ff4e8d20000 r-xp 00000000 08:02 140868                     /lib64/ld-2.14.1.so
7ff4e8ef3000-7ff4e8ef6000 rw-p 00000000 00:00 0
7ff4e8f1e000-7ff4e8f20000 rw-p 00000000 00:00 0
7ff4e8f20000-7ff4e8f21000 r--p 00020000 08:02 140868                     /lib64/ld-2.14.1.so
7ff4e8f21000-7ff4e8f22000 rw-p 00021000 08:02 140868                     /lib64/ld-2.14.1.so
7ff4e8f22000-7ff4e8f23000 rw-p 00000000 00:00 0
7ff4e8f23000-7ff4e8f2c000 r-xp 00000000 08:02 2097261                    /bin/ping
7ff4e912b000-7ff4e912c000 r--p 00008000 08:02 2097261                    /bin/ping
7ff4e912c000-7ff4e912d000 rw-p 00009000 08:02 2097261                    /bin/ping
7ff4e912d000-7ff4e9161000 rw-p 00000000 00:00 0                          [heap]
7fff92da5000-7fff92dc6000 rw-p 00000000 00:00 0                          [stack]
7fff92dff000-7fff92e00000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
netadmin:~ #
```

/home/tamas : bash /home/tamas : bash


/home/tamas : bash
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
netadmin:~ # cat /proc/self/maps
00400000-0040b000 r-xp 00000000 08:02 2097196 /bin/cat
0060a000-0060b000 r--p 0000a000 08:02 2097196 /bin/cat
0060b000-0060c000 rw-p 0000b000 08:02 2097196 /bin/cat
0060c000-0062d000 rw-p 00000000 00:00 0 [heap]
7f828b5a5000-7f828b72c000 r-xp 00000000 08:02 131095 /lib64/libc-2.14.1.so
7f828b72c000-7f828b92b000 ---p 00187000 08:02 131095 /lib64/libc-2.14.1.so
7f828b92b000-7f828b92f000 r--p 00186000 08:02 131095 /lib64/libc-2.14.1.so
7f828b92f000-7f828b930000 rw-p 0018a000 08:02 131095 /lib64/libc-2.14.1.so
7f828b930000-7f828b935000 rw-p 00000000 00:00 0
7f828b935000-7f828b955000 r-xp 00000000 08:02 140868 /lib64/ld-2.14.1.so
7f828bae9000-7f828bb28000 r--p 00000000 08:02 2761359 /usr/lib/locale/hu_HU.utf8/LC_CTYPE
7f828bb28000-7f828bb2b000 rw-p 00000000 00:00 0
7f828bb4d000-7f828bb54000 r--s 00000000 08:02 2637222 /usr/lib64/gconv/gconv-modules.cache
7f828bb54000-7f828bb55000 rw-p 00000000 00:00 0
7f828bb55000-7f828bb56000 r--p 00020000 08:02 140868 /lib64/ld-2.14.1.so
7f828bb56000-7f828bb57000 rw-p 00021000 08:02 140868 /lib64/ld-2.14.1.so
7f828bb57000-7f828bb58000 rw-p 00000000 00:00 0
7fff4b994000-7fff4b9b5000 rw-p 00000000 00:00 0 [stack]
7fff4b9ff000-7fff4ba00000 r-xp 00000000 00:00 0 [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0 [vsyscall]
netadmin:~ # objdump -f /bin/ping
/bin/ping: file format elf64-x86-64
architecture: i386:x86-64, flags 0x00000150:
HAS_SYMS, DYNAMIC, D_PAGED
start address 0x00000000000035f8
netadmin:~ # objdump -f /bin/cat
/bin/cat: file format elf64-x86-64
architecture: i386:x86-64, flags 0x00000112:
EXEC_P, HAS_SYMS, D_PAGED
start address 0x0000000000402808
netadmin:~ #
/home/tamas : bash
/home/tamas : bash

PaX védelemmel ellátott, és anélküli kernel vizsgálata a paxtest programmal:

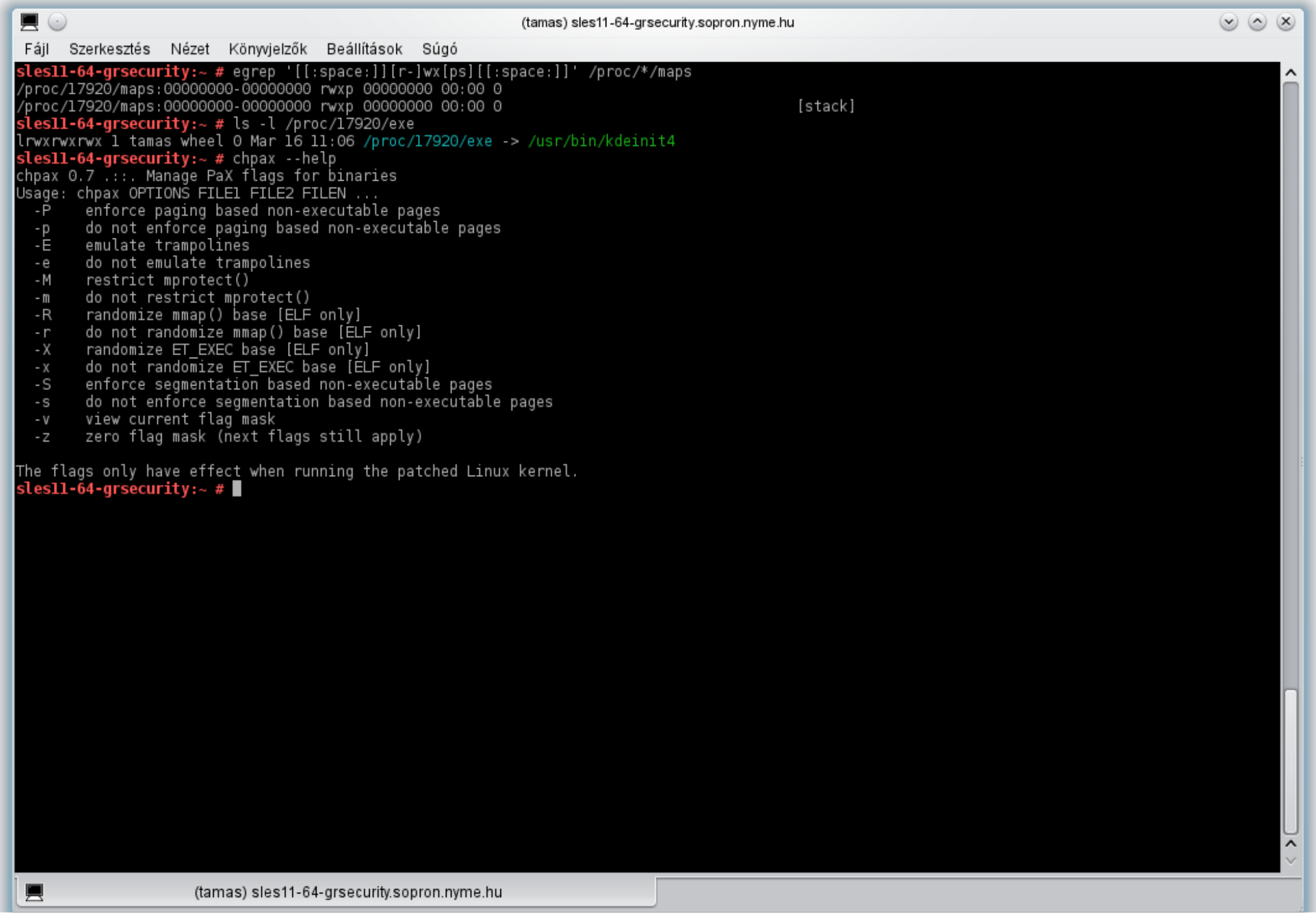
PaX nélkül:

```
Executable anonymous mapping : Killed
Executable bss : Killed
Executable data : Killed
Executable heap : Killed
Executable stack : Killed
Executable shared library bss : Killed
Executable shared library data : Killed
Executable anonymous mapping (mprotect) : Vulnerable
Executable bss (mprotect) : Vulnerable
Executable data (mprotect) : Vulnerable
Executable heap (mprotect) : Vulnerable
Executable stack (mprotect) : Vulnerable
Executable shared library bss (mprotect) : Vulnerable
Executable shared library data (mprotect): Vulnerable
Writable text segments : Vulnerable
Anonymous mapping randomisation test : 28 bits (guessed)
Heap randomisation test (ET_EXEC) : No randomisation
Heap randomisation test (PIE) : 28 bits (guessed)
Main executable randomisation (ET_EXEC) : No randomisation
Main executable randomisation (PIE) : 28 bits (guessed)
Shared library randomisation test : 28 bits (guessed)
Stack randomisation test (SEGMEXEC) : 28 bits (guessed)
Stack randomisation test (PAGEEXEC) : 28 bits (guessed)
Return to function (strcpy) :
paxtest: return address contains a NULL byte.
Return to function (memcpy) : Vulnerable
Return to function (strcpy, PIE) :
paxtest: return address contains a NULL byte.
Return to function (memcpy, PIE) : Vulnerable
```

PaXszal:

```
Executable anonymous mapping : Killed
Executable bss : Killed
Executable data : Killed
Executable heap : Killed
Executable stack : Killed
Executable shared library bss : Killed
Executable shared library data : Killed
Executable anonymous mapping (mprotect) : Killed
Executable bss (mprotect) : Killed
Executable data (mprotect) : Killed
Executable heap (mprotect) : Killed
Executable stack (mprotect) : Killed
Executable shared library bss (mprotect) : Killed
Executable shared library data (mprotect): Killed
Writable text segments : Killed
Anonymous mapping randomisation test : 33 bits (guessed)
Heap randomisation test (ET_EXEC) : 13 bits (guessed)
Heap randomisation test (PIE) : 40 bits (guessed)
Main executable randomisation (ET_EXEC) : No randomisation
Main executable randomisation (PIE) : 32 bits (guessed)
Shared library randomisation test : 33 bits (guessed)
Stack randomisation test (SEGMEXEC) : 40 bits (guessed)
Stack randomisation test (PAGEEXEC) : 40 bits (guessed)
Return to function (strcpy) :
paxtest: return address contains a NULL byte.
Return to function (memcpy) : Vulnerable
Return to function (strcpy, PIE) :
paxtest: return address contains a NULL byte.
Return to function (memcpy, PIE) : Vulnerable
```

A kékkel jelölt tesztek által vizsgált támadások ellen a PaX nem véd, viszont „korlátozott” védelmet nyújthatnak a GCC/GLibc SSP és FORTIFY_SOURCE opciói.


(tamas) sles11-64-grsecurity.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
sles11-64-grsecurity:~ # egrep '[[:space:]][r-]wx[ps][[:space:]]' /proc/*/maps
/proc/17920/maps:00000000-00000000 rwxp 00000000 00:00 0
/proc/17920/maps:00000000-00000000 rwxp 00000000 00:00 0 [stack]
sles11-64-grsecurity:~ # ls -l /proc/17920/exe
lrwxrwxrwx 1 tamas wheel 0 Mar 16 11:06 /proc/17920/exe -> /usr/bin/kdeinit4
sles11-64-grsecurity:~ # chpax --help
chpax 0.7 .::. Manage PaX flags for binaries
Usage: chpax OPTIONS FILE1 FILE2 FILEN ...
-P enforce paging based non-executable pages
-p do not enforce paging based non-executable pages
-E emulate trampolines
-e do not emulate trampolines
-M restrict mprotect()
-m do not restrict mprotect()
-R randomize mmap() base [ELF only]
-r do not randomize mmap() base [ELF only]
-X randomize ET_EXEC base [ELF only]
-x do not randomize ET_EXEC base [ELF only]
-S enforce segmentation based non-executable pages
-s do not enforce segmentation based non-executable pages
-v view current flag mask
-z zero flag mask (next flags still apply)
The flags only have effect when running the patched Linux kernel.
sles11-64-grsecurity:~ #
(tamas) sles11-64-grsecurity.sopron.nyme.hu

További PaX védelmi megoldások

- KERNEXEC : A NOEXEC kiterjesztése a kernelre

- UDEREF : Megakadályozza, hogy a kernelmódú utasításvégrehajtás felhasználói memóriaterületre tévedjen. (Nullpointer dereference)

- MEMORY_SANITIZE, STACKLEAK, REFCOUNT, USERCOPY, stb.

1. SELinux

-Eredeti fejlesztője a U.S. National Security Agency (NSA)

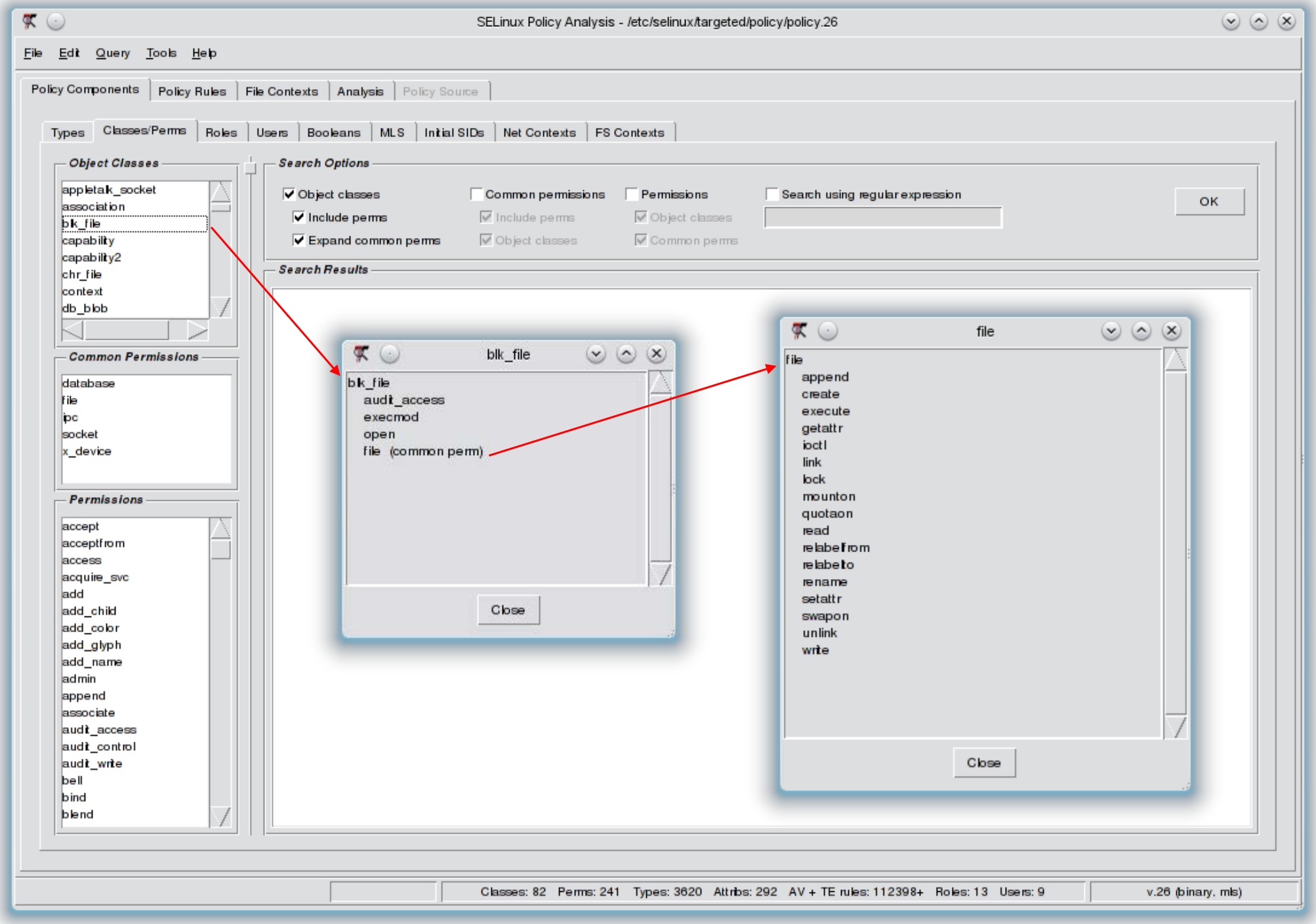
-Linux Security Modules (LSM) alapú MAC rendszer, ezért a kernel csak akkor hívja meg, ha a DAC engedélyez a műveletet, vagyis csak szigorításra ad lehetőséget

-A SELinux házirendje olyan szabályokból áll, amelyek meghatározzák, hogy adott „security context”-tel rendelkező szubjektum (processz) milyen engedélyekkel rendelkezik az adott osztályba (pl. fájl, blokkeszköz, processz, capability, netlink socket, stb...) tartozó objektumon.

-A policy főbb elemei:

-Type Enforcement / Role-based access control

-Multilevel security / Multi categories security


SELinux Policy Analysis - /etc/selinux/targeted/policy/policy.26
File Edit Query Tools Help
Policy Components Policy Rules File Contexts Analysis Policy Source
Types Classes/Perms Roles Users Booleans MLS Initial SIDs Net Contexts FS Contexts
Object Classes
appletalk_socket
association
blk_file
capability
capability2
chr_file
context
db_blob
Common Permissions
database
file
ipc
socket
x_device
Permissions
accept
acceptfrom
access
acquire_svc
add
add_child
add_color
add_glyph
add_name
admin
append
associate
audit_access
audit_control
audit_write
bell
bind
blend
Search Options
Object classes
Include perms
Expand common perms
Common permissions
Include perms
Object classes
Permissions
Object classes
Common perms
Search using regular expression
OK
Search Results
blk_file
blk_file
audit_access
execmod
open
file (common perm)
Close
file
file
append
create
execute
getattr
ioctl
link
lock
mounton
quotaon
read
relabelfrom
relabelto
rename
setattr
swapon
unlink
write
Close
Classes: 82 Perms: 241 Types: 3620 Attribs: 292 AV + TE rules: 112398+ Roles: 13 Users: 9
v.26 (binary, mls)

Szubjektum security context:

```
[root@fedora16 ~]# ps -Z
LABEL                             PID TTY          TIME CMD
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1388 pts/0 00:00:00 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1446 pts/0 00:00:17 tclsh
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 2045 pts/0 00:00:00 ps

user         role         type/domain  MLS/MCS range
```

Objektum security context:

```
[root@fedora16 ~]# ls -Z
-rw-------. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log.syslog

                     user     role     type         MLS/MCS label
```

A hozzáférésvezérlésben csak a type és az MLS/MCS értékek játszanak szerepet.

A Type Enforcement / Role-based access control szabályrendszer az explicit „allow” direktívákra épít.

A Multilevel security / Multi categories security szabályrendszer az eredeti Bell-LaPadula modellt (no read up; no write down) kis mértékben módosítja: (no read up; write equal)

(root) 172.23.6.158

Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó

```
[root@fedora16 ~]# ps -Z
LABEL                             PID TTY          TIME CMD
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1388 pts/0 00:00:00 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1446 pts/0 00:00:17 tclsh
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 2120 pts/0 00:00:00 ps
[root@fedora16 ~]# ls -Z
-rw-------. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log.syslog
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0:c1.c3 test
[root@fedora16 ~]# getfattr -m '.*' -d  install.log
# file: install.log
security.selinux="system_u:object_r:admin_home_t:s0"

[root@fedora16 ~]# cat /etc/selinux/targeted/seusers
system_u:system_u:s0-s0:c0.c1023
root:unconfined_u:s0-s0:c0.c1023
__default__:unconfined_u:s0-s0:c0.c1023
[root@fedora16 ~]# semanage user -l

                Címkézés   MLS/       MLS/
SELinux felhasználó Előtag     MCS Szint  MCS hatáskör                SELinux szerepek

git_shell_u     user       s0         s0                          git_shell_r
guest_u         user       s0         s0                          guest_r
root            user       s0         s0-s0:c0.c1023              staff_r sysadm_r system_r unconfined_r
staff_u         user       s0         s0-s0:c0.c1023              staff_r sysadm_r system_r unconfined_r
sysadm_u        user       s0         s0-s0:c0.c1023              sysadm_r
system_u        user       s0         s0-s0:c0.c1023              system_r unconfined_r
unconfined_u    user       s0         s0-s0:c0.c1023              system_r unconfined_r
user_u          user       s0         s0                          user_r
xguest_u        user       s0         s0                          xguest_r
[root@fedora16 ~]#
```

(root) 172.23.6.158 | ~ : bash | (root) sles11-64.sopron.nyme.hu

A szubjektumok és objektumok security context értéke teljesen független a UNIX/Linux metainformációktól (ortogonalitás)

A szubjektumok (proceszek) security context értéke type_transition szabályok alapján történik bináris fájlok végrehajtásakor, vagyis az általam elképzelt setuid+execve érzékenység közül csak az utóbbi valósul meg automatikusan.

A processzek – ha van hozzá joguk – maguk is válthatnak security context-et a /proc/PID/attr API-n keresztül a libselinux könyvtár segítségével.

A suid-érzékenység hiányosságát módosított (SELinux-érzékenyre patchelt, libselinuxszal linkelt) programcsomagokkal orvosolják, pl.: cron, logrotate, sshd, login, pam_unix(!) stb. A MAC rendszerekkel szemben támasztott feltételeim közül csak az első kettő teljesül, azok is csak speciális körülmények között.

A házirend bináris, forráskódból kell lefordítani. Az ortogonalitás miatt mindenképpen hamar kell betölteni a kernelbe, ezt a módosított init végzi.

Az audit2allow parancs segítségével „tanul”, azaz policy-forrást gyárt.

type_transition és feltételei:

```
# The rule states that when a process of type initrc_t executes
# a file of type acct_exec_t, the process type should be changed
 # to acct_t if allowed by the policy (i.e. Transition from the
            # initrc_t domain to the acc_t domain).

type_transition initrc_t acct_exec_t:process acct_t;

  # Note that to be able to transition to the acc_t domain the
    # following minimum permissions need to be granted in the policy
# using allow rules (as shown in the [#_allow_Rule allow Rule] section).

        # File needs to be executable in the initrc_t domain:
              allow initrc_t acct_exec_t:file execute;

     # The executable file needs an entry point into the acct_t
                              # domain:
              allow acct_t acct_exec_t:file entrypoint;

        # Process needs permission to transition into the acct_t domain:
              allow initrc_t acct_t:process transition;
```

Alapvetően kétféle policy: targeted és strict. A jóval egyszerűbb, alig szigorító targeted is több mint százezer allow szabályt tartalmaz :-(

2. RSBAC

-Eredeti fejlesztője Amon Ott.

-A SELinuxhoz hasonlóan inode alapú és ortogonális, de a fájlcímkéket nem xattr-okban tárolja, hanem minden a fájlrendszeren jelen levő `rsbac.dat` könyvtárakban bináris formában. Csak a kernel férhet hozzá, és folyamatosan aktualizálja.

-A policy nagy része a gyökérkönyvtár `rsbac.dat` könyvtárában van. Futásidőben szerkeszthető a „security” rendszerhíváson keresztül. Nem kell lefordítani, nem kell módosított init a betöltéséhez, mert a kernel tölti be.

-A `/etc/passwd`, `/etc/group` és `/etc/shadow` fájloknak a SELinuxnál is felmerülő cimkézési problémáit a pam_rsbac.so authentikációs modullal oldja meg. Ennél a megoldásnál a felhasználói adatbázis a kernel által felügyelt policy-ben van, az említett fájlokat akár törölni is lehet.

-Tanulási képességei korlátozottak.

Moduláris felépítésű

-AUTH: Meghatározza, mely processz mely UID-et, milyen GID-eket vehet fel. A login és hasonló binárisok számára beállítható pl., hogy csak a kernel által utoljára sikeresen autentikált felhasználó UID-jét vehessék fel.

-RC: Az RC modul a SELinux TE/RBAC szabályrendszeréhez hasonló policyt biztosít. A processzekhez a SELinux többtagú „security contex”-je helyett egy egyszerű szerepet (role) rendel. A szerepet a kernel a processz RUID-je és az utoljára végrehajtott binárishoz rendelt `rc_force_role` és `rc_initial_role` értékek alapján számítja ki, így a SELinuxszal szemben userland módosítás nélkül, tetszőleges szituációban használhatjuk „`type_transition`”-ként a setuid eseményeket, de a MAC rendszerekkel szemben támasztott követelményeim ugyanolyan korlátozottan érvényesülnek.

-ACL: Hozzáférés-vezérlő listákkal leírható policy-t biztosít.

-MAC: A SELinuxéhoz hasonló (no read up; write equal) MLS policy MCS tulajdonságok nélkül.

-PAX: A PaX által értelmezhető metainformációt rendel a binárisokhoz, de a chpax/`paxctl` parancsok által generált ELF fejlécek helyett az RSBAC saját házirendjében tárolja azokat.

-DAZ: Dazuko on-access vírusellenőrző felület.

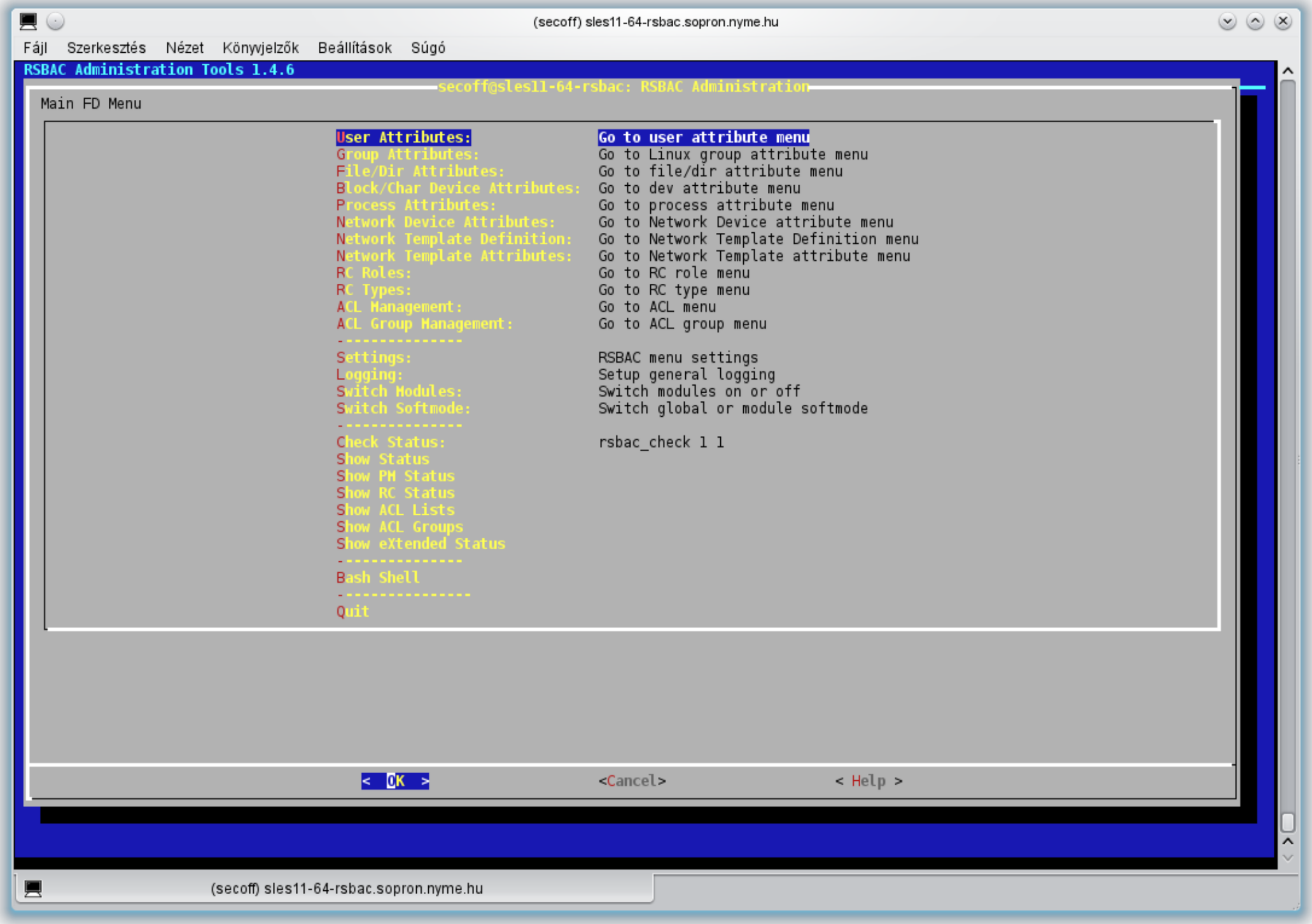
-CAP: A már említett filesystem capabilitykhez hasonlóan a root processzektől elvehet, a közönséges processzeknek adhat Linux capabilityket.

-JAIL: A `rsbac_jail` rendszerhíváson keresztül egy biztonsági célokra is hasonló chroot eszközt biztosít.

-RES: A processzek Linux erőforrásait szabályozza.

-FF: A `chattr` által beállítható Linux fájlattribútumokhoz hasonló hasznos flageket állíthatunk be a fájlokra.

-PM: Simone Fischer-Hübner biztonsági modellje. Egy újabb absztrakt biztonsági modell.

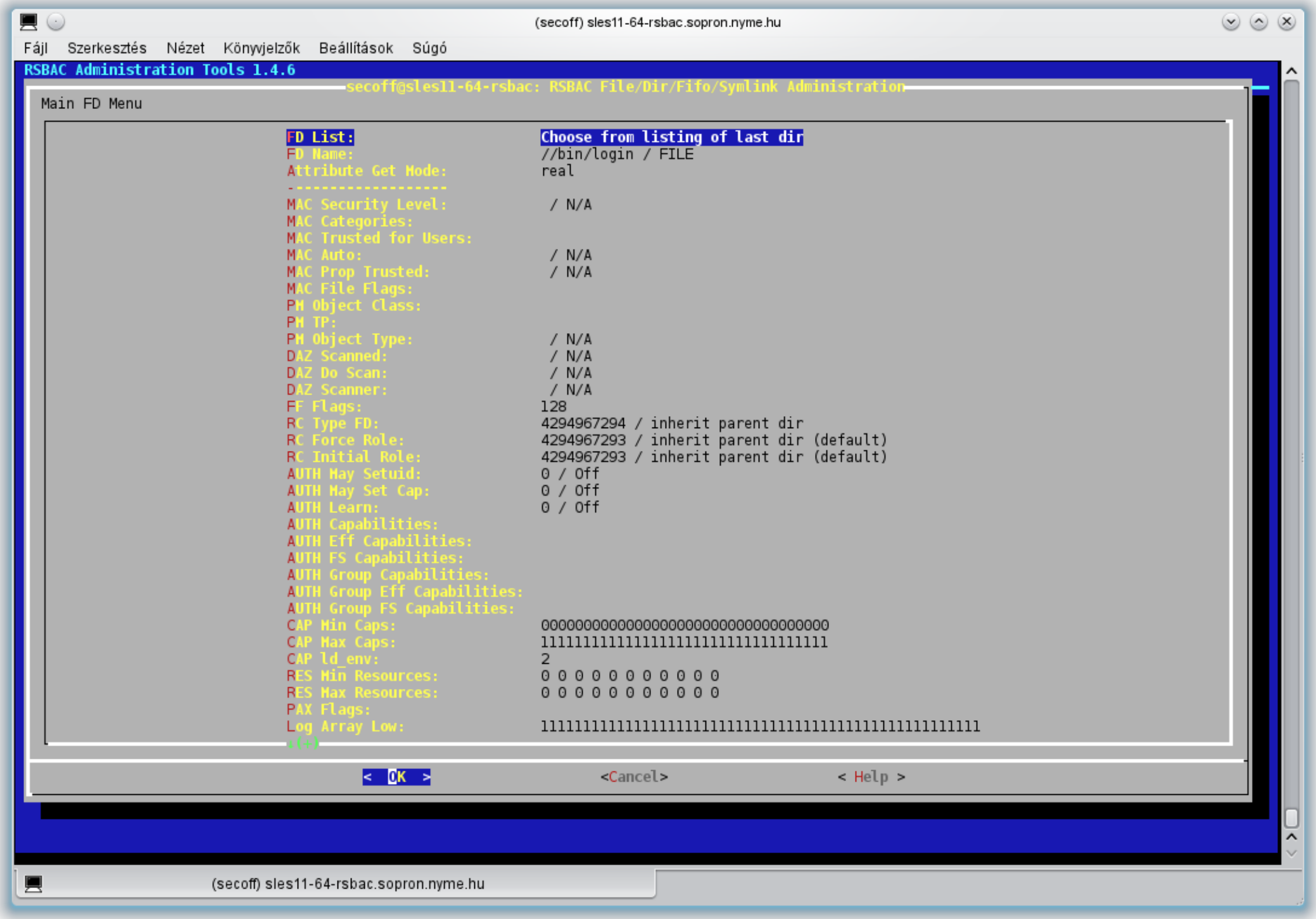

(secoff) sles11-64-rsbac.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
RSBAC Administration Tools 1.4.6
secoff@sles11-64-rsbac: RSBAC Administration
Main FD Menu
User Attributes: Go to user attribute menu
Group Attributes: Go to Linux group attribute menu
File/Dir Attributes: Go to file/dir attribute menu
Block/Char Device Attributes: Go to dev attribute menu
Process Attributes: Go to process attribute menu
Network Device Attributes: Go to Network Device attribute menu
Network Template Definition: Go to Network Template Definition menu
Network Template Attributes: Go to Network Template attribute menu
RC Roles: Go to RC role menu
RC Types: Go to RC type menu
ACL Management: Go to ACL menu
ACL Group Management: Go to ACL group menu

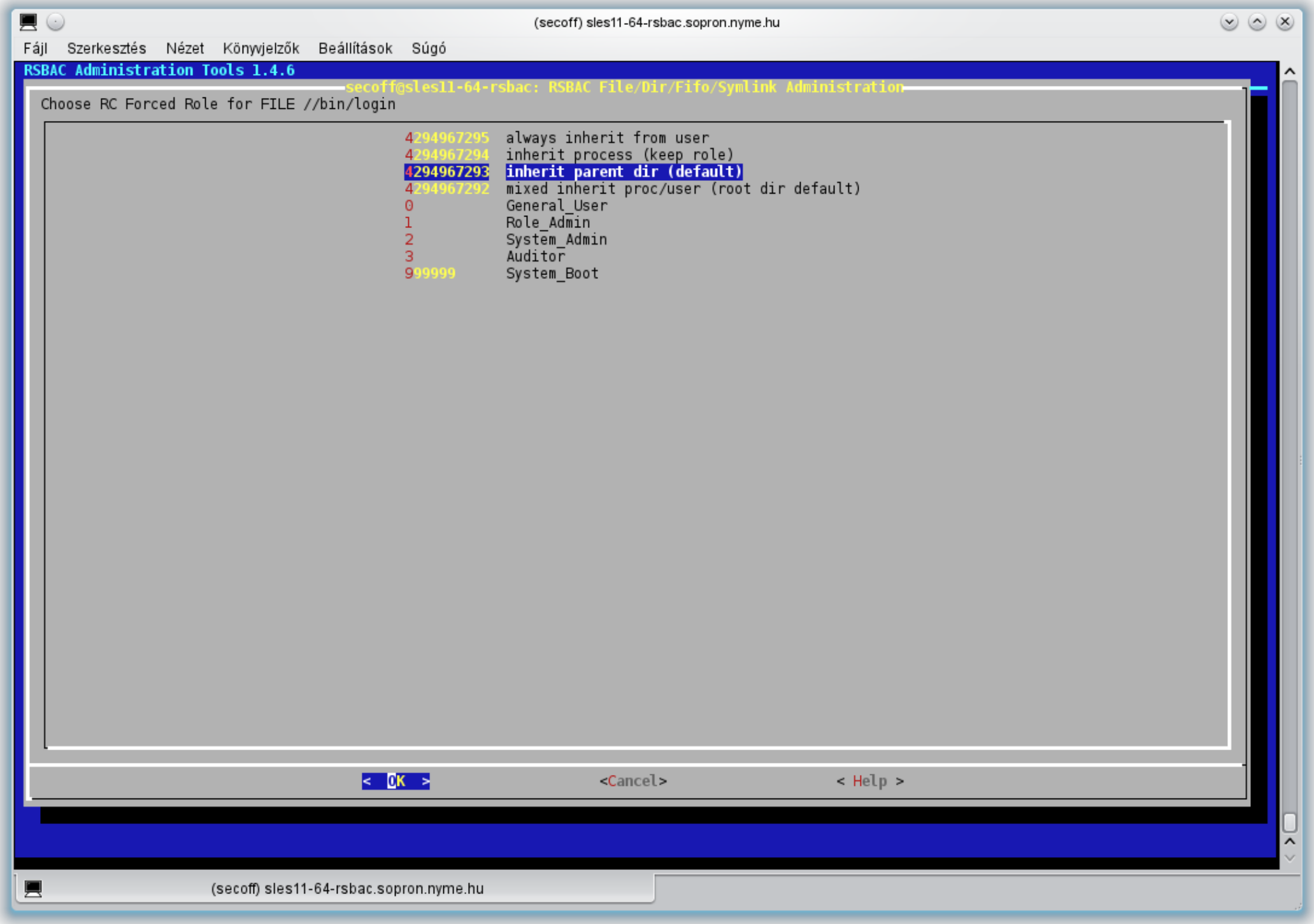
Settings: RSBAC menu settings
Logging: Setup general logging
Switch Modules: Switch modules on or off
Switch Softmode: Switch global or module softmode

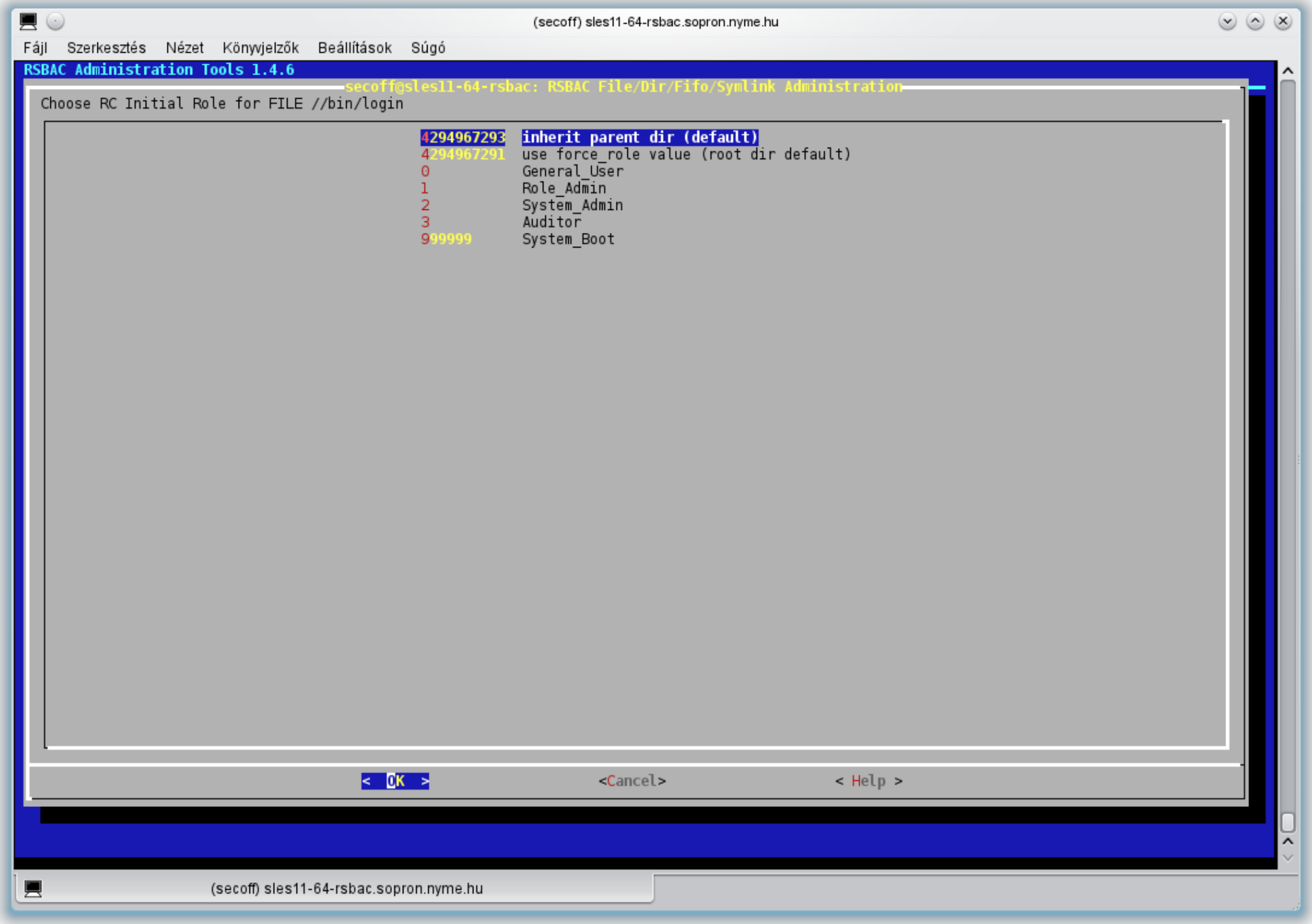
Check Status: rsbac_check 1 1
Show Status
Show PM Status
Show RC Status
Show ACL Lists
Show ACL Groups
Show eXtended Status

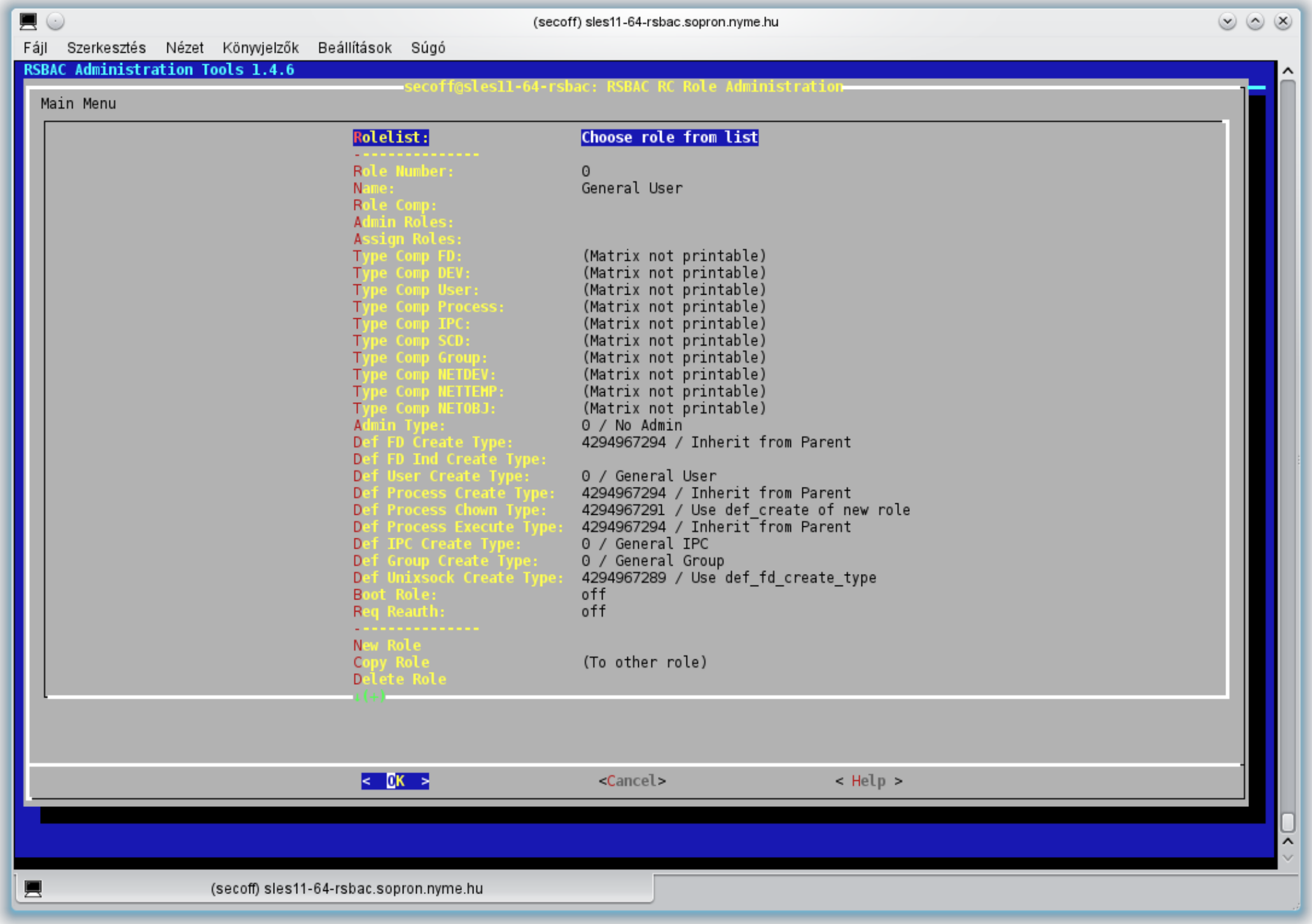
Bash Shell

Quit
< OK >
<Cancel>
< Help >
(secoff) sles11-64-rsbac.sopron.nyme.hu


(secoff) sles11-64-rsbac.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
RSBAC Administration Tools 1.4.6
secoff@sles11-64-rsbac: RSBAC File/Dir/Fifo/Symlink Administration
Main FD Menu
FD List: Choose from listing of last dir
FD Name: //bin/login / FILE
Attribute Get Mode: real
MAC Security Level: / N/A
MAC Categories:
MAC Trusted for Users:
MAC Auto: / N/A
MAC Prop Trusted: / N/A
MAC File Flags:
PM Object Class:
PM TP:
PM Object Type: / N/A
DAZ Scanned: / N/A
DAZ Do Scan: / N/A
DAZ Scanner: / N/A
FF Flags: 128
RC Type FD: 4294967294 / inherit parent dir
RC Force Role: 4294967293 / inherit parent dir (default)
RC Initial Role: 4294967293 / inherit parent dir (default)
AUTH May Setuid: 0 / Off
AUTH May Set Cap: 0 / Off
AUTH Learn: 0 / Off
AUTH Capabilities:
AUTH Eff Capabilities:
AUTH FS Capabilities:
AUTH Group Capabilities:
AUTH Group Eff Capabilities:
AUTH Group FS Capabilities:
CAP Min Caps: 00000000000000000000000000000000
CAP Max Caps: 11111111111111111111111111111111
CAP ld_env: 2
RES Min Resources: 0 0 0 0 0 0 0 0 0 0
RES Max Resources: 0 0 0 0 0 0 0 0 0 0
PAX Flags:
Log Array Low: 11111111111111111111111111111111111111111111111111111111
< OK >
<Cancel>
< Help >
(secoff) sles11-64-rsbac.sopron.nyme.hu


(secoff) sles11-64-rsbac.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
RSBAC Administration Tools 1.4.6
secoff@sles11-64-rsbac: RSBAC File/Dir/Fifo/Symlink Administration
Choose RC Forced Role for FILE //bin/login
4294967295 always inherit from user
4294967294 inherit process (keep role)
4294967293 inherit parent dir (default)
4294967292 mixed inherit proc/user (root dir default)
0 General_User
1 Role_Admin
2 System_Admin
3 Auditor
999999 System_Boot
< OK >
<Cancel>
< Help >
(secoff) sles11-64-rsbac.sopron.nyme.hu


(secoff) sles11-64-rsbac.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
RSBAC Administration Tools 1.4.6
secoff@sles11-64-rsbac: RSBAC File/Dir/Fifo/Symlink Administration
Choose RC Initial Role for FILE //bin/login
4294967293 inherit parent dir (default)
4294967291 use force_role value (root dir default)
0 General_User
1 Role_Admin
2 System_Admin
3 Auditor
999999 System_Boot
< OK >
<Cancel>
< Help >
(secoff) sles11-64-rsbac.sopron.nyme.hu


(secoff) sles11-64-rsbac.sopron.nyme.hu
Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó
RSBAC Administration Tools 1.4.6
secoff@sles11-64-rsbac: RSBAC RC Role Administration
Main Menu
Rolelist: Choose role from list
Role Number: 0
Name: General User
Role Comp:
Admin Roles:
Assign Roles:
Type Comp FD: (Matrix not printable)
Type Comp DEV: (Matrix not printable)
Type Comp User: (Matrix not printable)
Type Comp Process: (Matrix not printable)
Type Comp IPC: (Matrix not printable)
Type Comp SCD: (Matrix not printable)
Type Comp Group: (Matrix not printable)
Type Comp NETDEV: (Matrix not printable)
Type Comp NETTEMP: (Matrix not printable)
Type Comp NETOBJ: (Matrix not printable)
Admin Type: 0 / No Admin
Def FD Create Type: 4294967294 / Inherit from Parent
Def FD Ind Create Type:
Def User Create Type: 0 / General User
Def Process Create Type: 4294967294 / Inherit from Parent
Def Process Chown Type: 4294967291 / Use def_create of new role
Def Process Execute Type: 4294967294 / Inherit from Parent
Def IPC Create Type: 0 / General IPC
Def Group Create Type: 0 / General Group
Def Unixsock Create Type: 4294967289 / Use def_fd_create_type
Boot Role: off
Req Reauth: off
New Role
Copy Role (To other role)
Delete Role
< OK > <Cancel> < Help >
(secoff) sles11-64-rsbac.sopron.nyme.hu

A MAC biztonsági házirenden kívül rengeteg egyéb biztonsági megoldást kínál:

-A már említett kernelbeli felhasználói adatbázis

-Opcionális PaX integráció (ún. enhanced kernelek esetén)

-Érzékeny kerneladatok elrejtése

-UID, RC role, MAC level alapú symlink átirányítás

-stb.

3. AppArmor

- Eredetileg egy Immunix nevű cég fejlesztette SubDomain néven eredetileg nem LSM alapú volt, de portolták rá. A Novell megvette az Immunixet és az AppArmor névre váltott. Később a fejlesztőket elbocsátották és tisztán közösségivé vált a projekt, amíg az Ubuntut fejlesztő Canonical át nem vette.

- Ortogonalitás nincs, a SELinuxtól és az RSBAC-tól eltérően nem absztrakt típus, domain vagy szerep címkékkel osztályozza a szubjektumokat és objektumokat, hanem rendszerközeli UNIX metainformációkkal.

- A fájlokat nem inode, hanem elérési út (pathname) alapján különbözteti meg. Az AppArmor teljesen fájlrendszer-független.

- A bemutatott négy rendszer közül ez az egyetlen, amelynél „mindent szabad, amit nem tilos”.

- A házirend bármikor betölthető vagy kikapcsolható.

- Az AppArmor konfigurációja és házirendje a `/etc/apparmor` könyvtárban található. Szöveges formátumú, lefordítani nem kell, az `apparmor_parser` ezt betöltés közben elvégzi.

- `aa-genprof` néven automatikus profilgeneráló eszközzel is rendelkezik.

http://wiki.apparmor.net/index.php/AppArmor_Core_Policy_Reference

```
/usr/local/example_executable {
  #include <abstractions/base>

  capability net_raw,

     /usr/local/example_executable rmix,
     /etc/networks r,
     @{PROC} r,
     owner @{PROC}/*/net/raw r,
     /bin/exec2   cx,
     ...

     ^hat_1 {
         # aa_change_hat rendszerhívás számára
         ...
     }


     /bin/exec2 {
     ..

     }
 }
```

Ez a policy szintaxis csak olyan házirendek készítését teszi lehetővé, amelyek execve-érzékenyen, de nem suid-érzékenyen állítják be a processzek jogosultságait.

A pam_apparmor.so modul segítségével az azt felhasználó autentikáló programok automatikusan profilt válthatnak bejelentkező felhasználó neve vagy csoportja alapján az aa_change_hat rendszerhívás segítségével.

Ezzel az AppArmor korlátozottan RBAC/MAC viselkedésemulációjára képes, és PAM session-öket támogató cron démon segítségével elsőként teljesíti komplikációk nélkül a MAC rendszerekkel szemben támasztott követelményeimet, de lehetne általánosabb és userland-függetlenebb is...

4. Grsecurity

- Fejlesztője Brad Splengler

- Az RSBAC-hoz hasonlóan nem LSM alapú, és nem része a vanilla kernelnek

- Az AppArmohoz hasonlóan nincs ortogonalitás, és absztrakt biztonsági cimkék helyett meglevő UNIX fogalmak alapján osztályozza az szubjekteket és objekteket.

- Az AppArmohoz hasonlóan nem inode, hanem elérési út alapú házirend.

- Az AppArmorral szemben „mindent tilos, amit nem szabad” alapelvű, de amikor a policy nincs betöltve, akkor akkor mindent szabad, ezért a `/etc/grsec` könyvtárban található házirend bármikor betölthető. Különböző elképzelések vannak arról, hogy a boot folyamat elején vagy végén érdemes betölteni.

- Házirend-szintaxisa az AppArmoréhoz hasonló, de kétszintű. A külső szinten a az UID/GID alapú „role”kategóriák vannak, a belső szinten pedig a binárisfájl-alapú „subject” kategóriák, amelyek az AppArmor „profile” fogalmához hasonlóan működnek.

- Az egyszerű szintaxis ellenére ez az első megoldás, ami maradéktalanul, bármilyen körülmények között, semmilyen userland segítséget nem igényelve teljesíti a MAC rendszerekkel szemben támasztott kívánalmaimat. A Grsecurity userland-ja mindössze három végrehajtható fájlból, egy man oldalból, és a konfigurációt tartalmazó /etc/grsec könyvtárból áll.

- Tanuló üzemmódja annyira hatékony, hogy emberi közreműködés nélkül képes a SELinux „strict” házirendjéhez hasonlóan erős védelmet biztosító policy létrehozására.

- PaX nélkül nincs Grsecurity, sőt, mivel a Grsecurityben levő PaX forráskód frissebb, mint a különálló, azt is mondhatjuk, hogy Grsecurity nélkül nincs PaX

- A Grsecurity használata nem szokatlan az RSBAC (MAC) rendszer nélkül, mivel számos kiegészítő biztonsági megoldással rendelkezik, pl.
  - PaX
  - TPE – csak root tulajdonú, root által írható könyvtárakban levő programok indítását engedélyezi.
  - Véletlenszerűség növelése
  - Adatszivárgás elleni védelmek (/proc, /sys, dmesg, stb.)
  - Erőteljes védelem a futó kernel módosítása ellen
  - A chroot rendszerhívás biztonsági megoldássá fejlesztése
  - Bruteforce támadás alatt álló processzek forkolásának letiltása (PaX alapján)
  - Kernel exploitot futtató felhasználó kizárása (PaX alapján)
  - stb.

(AD\nice) u-96.sopron.nyme.hu

Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó

```
sles11-64-grsecurity:~ # ls -l /dev/grsec
crw--w--w- 1 root root 1, 13 2013-03-21 12:27 /dev/grsec
sles11-64-grsecurity:~ # ls -la /proc/sys/kernel/grsecurity
total 0
dr-x------ 0 root root 0 2013-03-21 12:27 .
dr-xr-xr-x 0 root root 0 2013-03-21 12:27 ..
-rw------- 1 root root 0 2013-03-21 12:27 audit_chdir
-rw------- 1 root root 0 2013-03-21 12:27 audit_mount
-rw------- 1 root root 0 2013-03-21 12:27 audit_ptrace
-rw------- 1 root root 0 2013-03-21 12:27 chroot_caps
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_chmod
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_chroot
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_fchdir
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_mknod
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_mount
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_pivot
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_shmat
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_sysctl
-rw------- 1 root root 0 2013-03-21 12:27 chroot_deny_unix
-rw------- 1 root root 0 2013-03-21 12:27 chroot_enforce_chdir
-rw------- 1 root root 0 2013-03-21 12:27 chroot_execlog
-rw------- 1 root root 0 2013-03-21 12:27 chroot_findtask
-rw------- 1 root root 0 2013-03-21 12:27 chroot_restrict_nice
-rw------- 1 root root 0 2013-03-21 12:27 consistent_setxid
-rw------- 1 root root 0 2013-03-21 12:27 deter_bruteforce
-rw------- 1 root root 0 2013-03-21 12:27 dmesg
-rw------- 1 root root 0 2013-03-21 12:27 exec_logging
-rw------- 1 root root 0 2013-03-21 12:27 fifo_restrictions
-rw------- 1 root root 0 2013-03-21 12:27 forkfail_logging
-rw------- 1 root root 0 2013-03-21 12:27 grsec_lock
-rw------- 1 root root 0 2013-03-21 12:27 harden_ptrace
-rw------- 1 root root 0 2013-03-21 12:27 linking_restrictions
-rw------- 1 root root 0 2013-03-21 12:27 ptrace_readexec
-rw------- 1 root root 0 2013-03-21 12:27 resource_logging
-rw------- 1 root root 0 2013-03-21 12:27 romount_protect
-rw------- 1 root root 0 2013-03-21 12:27 rwxmap_logging
-rw------- 1 root root 0 2013-03-21 12:27 signal_logging
-rw------- 1 root root 0 2013-03-21 12:27 timechange_logging
-rw------- 1 root root 0 2013-03-21 12:27 tpe
-rw------- 1 root root 0 2013-03-21 12:27 tpe_gid
-rw------- 1 root root 0 2013-03-21 12:27 tpe_invert
sles11-64-grsecurity:~ #
```

(AD\nice) u-96.sopron.nyme.hu

(AD\nice) u-96.sopron.nyme.hu

Fájl Szerkesztés Nézet Könyvjelzők Beállítások Súgó

```
sles11-64-grsecurity:/etc/grsec # gradm -P
Setting up grsecurity RBAC password
Password:
Re-enter Password:
Password written to /etc/grsec/pw.
sles11-64-grsecurity:/etc/grsec # gradm -F -L /etc/grsec/learning.logs2
sles11-64-grsecurity:/etc/grsec # gradm -D
Password:
sles11-64-grsecurity:/etc/grsec # gradm -F -L /etc/grsec/learning.logs2 -O /etc/grsec/policy2
Beginning full learning 1st pass...done.
Beginning full learning role reduction...done.
Beginning full learning 2nd pass...done.
Beginning full learning subject reduction for user tamas...done.
Beginning full learning subject reduction for user root...done.
Beginning full learning subject reduction for user sshd...done.
Beginning full learning subject reduction for user postfix...done.
Beginning full learning object reduction for subject /...done.
Beginning full learning object reduction for subject /bin/bash...done.
Beginning full learning object reduction for subject /usr/bin/id...done.
Beginning full learning object reduction for subject /usr/bin/mc...done.
Beginning full learning object reduction for subject /usr/sbin/sshd...done.
Beginning full learning object reduction for subject /...done.
Beginning full learning object reduction for subject /bin/bash...done.
Beginning full learning object reduction for subject /bin/ls...done.
Beginning full learning object reduction for subject /usr/bin/id...done.
Beginning full learning object reduction for subject /usr/bin/mc...done.
Beginning full learning object reduction for subject /usr/bin/pstree...done.
Beginning full learning object reduction for subject /usr/lib/postfix/master...done.
Beginning full learning object reduction for subject /usr/lib64/mc/cons.saver...done.
Beginning full learning object reduction for subject /usr/sbin/nscd...done.
Beginning full learning object reduction for subject /usr/sbin/sshd...done.
Beginning full learning object reduction for subject /...done.
Full learning complete.
sles11-64-grsecurity:/etc/grsec # gradm -E -L /etc/grsec/policy2
sles11-64-grsecurity:/etc/grsec # halt
-bash: /proc/self/stat: Permission denied
-bash: test: 3602: unary operator expected
If 'halt' is not a typo you can run the following command to lookup the package that contains the binary:
    command-not-found halt
-bash: halt: command not found
sles11-64-grsecurity:/etc/grsec # gradm -a admin
Password:
sles11-64-grsecurity:/etc/grsec # halt

Broadcast message from root (pts/0) (Thu Mar 21 12:26:11 2013):

The system is going down for system halt NOW!
```

(AD\nice) u-96.sopron.nyme.hu

```
define grsec_denied {
        /boot   h
        /dev/grsec      h
        /dev/kmem       h
        /dev/port       h
        /etc/grsec      h
        /proc/kcore     h
        /proc/modules   h
        /lib/modules    hs
        /etc/ssh        h
}

role admin sAP
subject / rvka
        / rwcdmlxi

role shutdown sARG
subject / rvka
        /
        /dev
        /dev/urandom r
        /dev/random r
        /etc r
        /bin rx
        /sbin rx
        /lib rx
        /lib64 rx
        /usr rx
        /proc r
        $grsec_denied
        -CAP_ALL
        connect disabled
        bind disabled

role default
subject /
        /                       h
        -CAP_ALL
        connect disabled
        bind    disabled
```

```
role root uG
role_transitions admin shutdown

subject /usr/sbin/sshd o {
        /
        /bin                                h
        /bin/bash                           x
        /boot                               h
        /dev                                h
        /dev/log                            rw
        /dev/null                           rw
        /dev/tty                            rw
        /dev/urandom                        r
        /etc                                r
        /etc/grsec                          h
        /lib/modules                        h
        /proc                               w
        /proc/bus                           h
        /proc/kcore                         h
        /proc/sys/kernel/ngroups_max        r
        /sys                                h
        /usr                                h
        /usr/sbin                           h
        /usr/sbin/sshd                      x
        /var                                h
        /var/lib/empty
        /var/log/lastlog                    rw
        /var/log/wtmp                       w
        /var/run/utmp                       rw
        -CAP_ALL
        +CAP_CHOWN
        +CAP_SETGID
        +CAP_SETUID
        +CAP_SYS_CHROOT
        +CAP_AUDIT_WRITE
        bind 0.0.0.0/32:22 stream dgram hopopt tcp
        bind 0.0.0.0/32:0 stream dgram hopopt tcp
        connect 193.225.93.1/32:53 dgram udp
        sock_allow_family ipv6 netlink
}
```

http://hup.hu/node/108217