

LUT School of Engineering Science

CT30A3370 Käyttöjärjestelmät ja systeemiohjelmointi

Harjoitustyö: Project 3: Kernel Hacking

Project 3

Kernel Hacking

15.12.2019

Tero Nevalainen 0521595

SISÄLLYSLUETTELO

1	Johdanto	1
2	Toiminta.....	1
3	Kuva toiminnasta	2

1 JOHDANTO

Tehtävänä oli tehdä oma system call xv6:seen, joka kertoo, kuinka monta kertaa read() funktiota on kutsuttu siitä lähtien kun, kernel bootattiin. Xv6 tiedostot latasin <https://github.com/mit-pdos/xv6-public> ja kaikki itse työ: <https://github.com/teronevalainen/project3-kernel>.

2 TOIMINTA

Xv6 tiedostoista muokkasin seuraavia: syscall.h, user.h, usys.S, syscall.c, sysproc.c, defs.h ja sysfile.c, lisäksi tein oman tiedoston **luku.c**.

Näihin tiedostoihin tein seuraavia muutoksia:

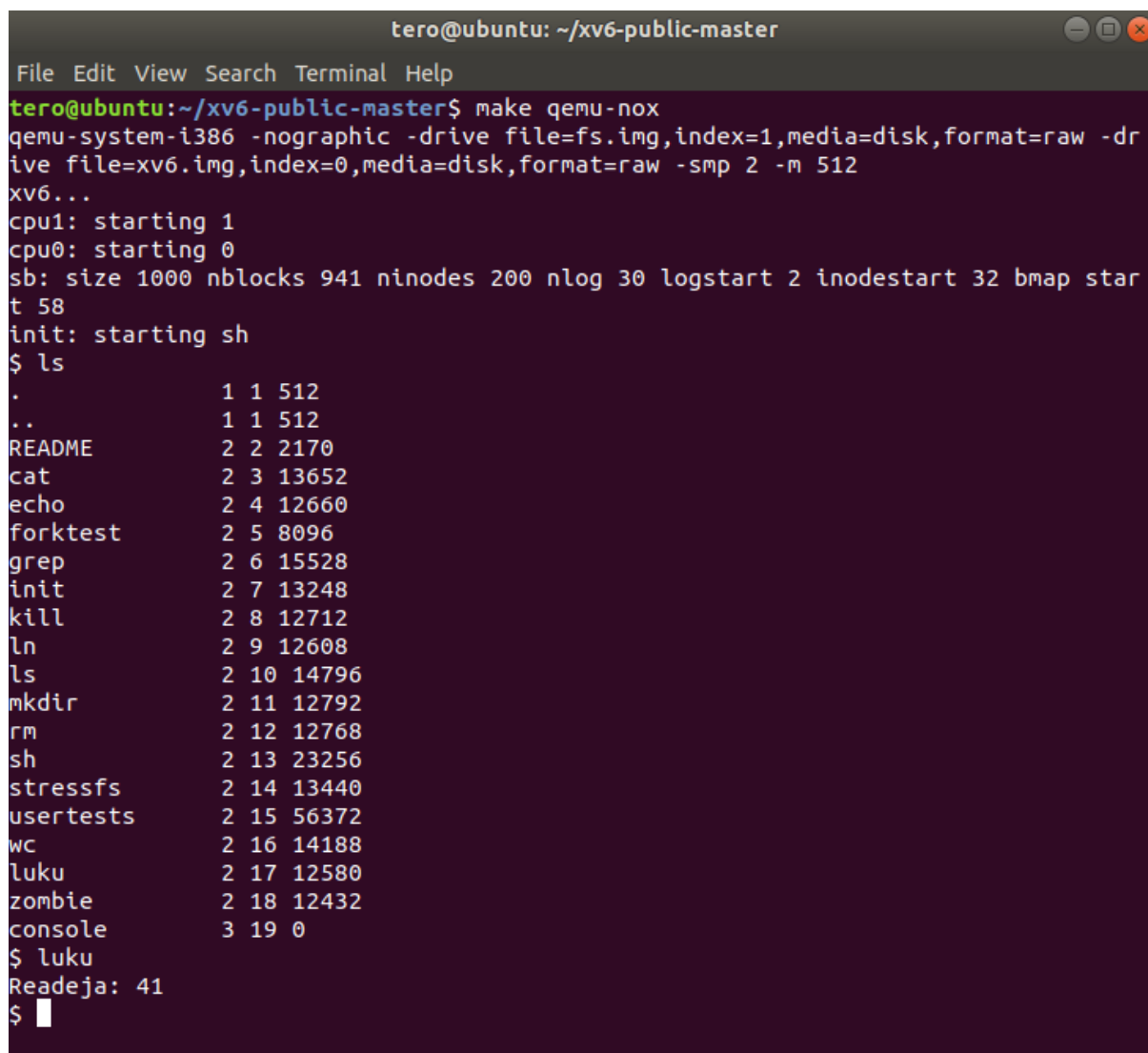
- syscall.h → #define SYS_getreadcount 22 eli määritin uuden järjestelmäkutsun numeron
- user.h → system calleihin: int getreadcount(void) eli uuden funktion määrittely
- usys.S → SYSCALL(getreadcount) uusi järjestelmäkutsu
- syscall.c → extern int sys_getreadcount(void) ja [SYS_getreadcount] sys_getreadcount
- sysproc.c → int sys_getreadcount(void){return getreadcount();}, palauttaa saamansa funktion
- defs.h → int getreadcount(void) proc.c kohtaan, funktion määrittely.
- sysfile.c → määritin int readmaaran, jonka laitoin myös sys_read() sisälle, joka siellä lisää itseään yhdellä joka kerta kun readia käytetään. Sen jälkeen tein uuden getreadcount(void) funktion ja se palauttaa luku.c:hen readmaaran arvon.

Tässä luku.c, joka printtaa readit:

```
1 #include "types.h"
2 #include "stat.h"
3 #include "user.h"
4
5 int main(int argc, char *argv[]) {
6     int luku = getreadcount();
7     printf(1, "Readeja: %d\n", luku);
8     exit();
9 }
```

Ohjelma kääntyy komennolla `make` ja käynnistuu komennolla `make qemu-nox`, jolloin ohjelma ei aukaise qemua erilliseen ikkunaan vaan pystytään käyttämään terminaalissa. Ajetaan komennolla `luku`.

3 KUVA TOIMINNASTA



```
tero@ubuntu: ~/xv6-public-master
File Edit View Search Terminal Help
tero@ubuntu:~/xv6-public-master$ make qemu-nox
qemu-system-i386 -nographic -drive file=fs.img,index=1,media=disk,format=raw -dr
ive file=xv6.img,index=0,media=disk,format=raw -smp 2 -m 512
xv6...
cpu1: starting 1
cpu0: starting 0
sb: size 1000 nblocks 941 ninodes 200 nlog 30 logstart 2 inodestart 32 bmap star
t 58
init: starting sh
$ ls
.          1 1 512
..         1 1 512
README    2 2 2170
cat        2 3 13652
echo       2 4 12660
forktest   2 5 8096
grep       2 6 15528
init       2 7 13248
kill       2 8 12712
ln         2 9 12608
ls         2 10 14796
mkdir      2 11 12792
rm         2 12 12768
sh         2 13 23256
stressfs   2 14 13440
usertests  2 15 56372
wc         2 16 14188
luku       2 17 12580
zombie     2 18 12432
console    3 19 0
$ luku
Readeja: 41
$
```

Komennolla `ls` näkee, että `luku` kuuluu järjestelmäkutsuihin ja se ajetaan komennolla `luku`.